Children's privacy in the online playground

Macenaite, Milda

Publication date:
2017

Document Version
Publisher's PDF, also known as Version of record

Children's Privacy in the Online Playground:

Dilemmas and Unresolved Challenges for EU Child-Specific Privacy Protection

Milda Mačėnaitė

Cover Photo: Robin Pierre on Unsplash

Children's privacy in the online playground:

Dilemmas and unresolved challenges for EU child-specific privacy protection

Milda Mačėnaitė

Children's privacy in the online playground:

Dilemmas and unresolved challenges for EU child-specific privacy protection

Proefschrift ter verkrijging van de graad van doctor aan Tilburg University op gezag van de rector magnificus, prof. dr. E.H.L. Aarts, in het openbaar te verdedigen ten overstaan van een door het college voor promoties aangewezen commissie in de aula van de Universiteit

op woensdag 29 november 2017 om 10.00 uur

door Milda Mačėnaitė, geboren op 3 maart 1983 te Vilnius, Litouwen

Promotores:

Prof. dr. J.E.J. Prins
Prof. dr. E. Kosta

Commmissieleden:

Prof. dr. R.E. Leenes
Prof. dr. E. Lievens
Prof. V. Steeves
Prof. dr. mr. S. van der Hof
Prof.mr. P. Vlaardingerbroek

Table of contents

Abbreviations

CNIL	La Commission Nationale de l'Informatique et des Libertés (French DPA)
COPPA	Children's Online Privacy Protection Act
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EC	European Commission
EDPS	European Data Protection Supervisor
ENISA	Agency for Network and Information Security
EU	European Union
FEDMA	Federation of European Direct and Interactive Marketing
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ICO	Information Commissioner’s Office (UK)
PRIAM	Privacy Risk Analysis Methodology
SNS	Social Networking Site
OFCOM	Office of Communications (UK)
UN CRC	United Nations Convention on the Rights of the Child

1. Introduction

Children are actively present online at an increasingly young age. It is estimated, that two in every ten internet users in the EU are under the age of 18[1] and children start using diverse internet-enabled devices, such as tablets and smartphones, when they are still infants.[2] As the internet has become "embedded, embodied and everyday"[3], the online and the offline are now seamlessly intertwined for children. The digital space is "just another setting in which they carry out their lives"[4].

Although the online playground does not offer the nostalgia-ridden outdoor pleasures associated with a happy childhood, such as splashing in puddles, making daisy chains and climbing trees, children nevertheless enjoy exciting opportunities online. They create, learn, self-express, experiment with relationships and identities and thereby developing as persons in the own right. Online services provide unprecedented benefits. For example, first, self-representation through the sharing personal life details with others and the forming an identity(ies).[5] Second, self-tracking which allows children to control their performance and self-improvement.[6] Third, playing videogames encourages children to develop their math, spatial reasoning, logic and readings skills.[7] And finally fourth, more generally children's involvement with digital media helps them to exercise their rights to information, education and participation.[8] Yet, there are also possible negative ramifications associated with active online engagement which put children's wellbeing and rights at risk.[9] Such risks can be broadly

---

1 Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' Global Commission on Internet Governance Paper Series No. 22, 2015.

2 Donell Holloway, Lelia Green and Sonia Livingstone, *Zero to eight: young children and their internet use.* EU Kids Online, LSE London, UK, 2013. See also OFCOM report on the empirical data collected in the UK, which shows that 16% of 3-4 year old children have their own tablet, and this number doubles for 5-7 year olds. OFCOM, Children and parents: media use and attitudes report 2016, 3 February 2017, available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-parents-nov16

3 Christine Hine, *Ethnography for the Internet: Embedded, Embodied and Everyday*. London: Bloomsbury, 2015.

4 Amanda Third et al., 'Children's Rights in the Digital Age: A Download from Children Around the World', Young and Well Cooperative Research Centre, Melbourne, 2014, 8.

5 Theresa Sauter, 'What's on your mind?' Writing on Facebook as a tool for self-formation. New Media & Society 16(5): 823–839, 2014. Alice E. Marwick, The public domain: social surveillance in everyday life. Surveillance & Society 9(4): 378–393, 2012.

6 Deborah Lupton, The Quantified Self: A Sociology of Self-tracking. Cambridge: Polity Press, 2016. Deborah Lupton, Digital bodies. In: Andrews D, Silk M and Thorpe H (eds) Routledge Handbook of Physical Cultural Studies. London: Routledge, 200–208, 2017.

7 Brecht Vandenbroucke, How Videogames Like *Minecraft* Actually Help Kids Learn to Read, 10 September 2014, availabe at: https://www.wired.com/2014/10/video-game-literacy/

8 Sonia Livingstone, Reframing media effects in terms of children's rights in the digital age. Journal of Children and Media 10(1): 4–12, 2016.

9 There are many different clasifications of online privacy risks. For an overview see D. Haynes and L. Robinson, Defining User Risk in Social Networking Services. Aslib Journal of Information Management, 67(1), 94-115, 2015. The EDPS has summarized the risks specifically for children as follows: "The growing use of the digital environment by children and the constant evolution of that environment pose new data protection and privacy risks (…). Such risks include, amongst others, misuse of their personal data, the unwanted dissemination of their personal profile on social networking sites, their growing use of geo-location services, their being increasingly directly subject to advertising campaigns and to serious crimes such as child abuse. These are particular risks that must be addressed in a manner appropriate to the specificity and vulnerability of the category of individuals at risk". EDPS (2012), Opinion on the Communication from the

framed as having two distinct dimensions: the first is the intense and pervasive personal data processing by companies (the user to company dimension) and the second being personal data misuse by other users (the user to user dimension). It is important to clarify that in reality the picture is more complicated. There could also be a third hybrid dimension which would cater for grey areas such as those related the potential fallibility of security protocols and the storage of personal data which may have both a user (criminal) to company and user (criminal) to user dimensions or a combination thereof. Although commercial data collection is a predominant feature online, personal data is also processed by public institutions and law enforcement agencies. The key point is that in practice the delineation of the dimensions is complicated but that for the purposes of this dissertation the line can be drawn given the particular purpose of the study.

As to the first dimension, the digital space is increasingly data-driven, hyper-connected and commercialised.[10] To be fully present and to interact with friends and commercial service providers via wearable and mobile devices or social media platforms, children often disclose their personal data. Such disclosure can occur intentionally or unintentionally *inter alia* when children sign up for online services, such as games or chats, or share their pictures on social media. Indeed, data collection online has become ubiquitous and remains often unnoticed: behaviour data, such as the websites visited, the words typed or even the mouse movements, can be easily collected via cookies, web beacons or through the increasingly used cross-device tracking techniques.[11] Also, the rise of Internet-connected devices, such as smart toys or wearable devices, allows for the continuous generation data which can be harvested for commercial interests and used to take decisions about individuals, including children. Collection of meta-data, such as the device type, usage or location data, by app providers is another relevant example of possible unnoticed data disclosure. Empirical research has demonstrated pervasive tracking occurring in the apps used by children.[12] The use of data analytics to infer new data and correlations from collected behavioural and meta-data has further amplified datafication.

As the second dimension reveals, increased data disclosures and sharing online might bring privacy issues not only due to the monetisation of data by companies but also due to potential data misuse and harms inflicted between individuals. Media outlets regularly report on cases related to the victimisation of internet users through the posting of personal details or indeed how such posts can go viral in the online setting thereby leaving individuals helpless to control their negative impact.[13] This can result in potential reputational loss, psychological

---

Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", 17 July 2012, para. 7.

[10] Simone van der Hof, I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World, 34 Wis. Int'l L.J. 2016.

[11] More on the latest tracking techniques and their potential impact on consumers see FTC Staff Report, Cross-Device Tracking, January 2017, available at: https://www.ftc.gov/system/files/documents/reports/cross-device-tracking-federal-trade-commission-staff-report-january-2017/ftc_cross-device_tracking_report_1-23-17.pdf

[12] Irwin Reyes et al., Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations, 2017, available at: http://eprints.networks.imdea.org/1557/1/conpro.pdf (the authors discovered that "over 80% of the apps potentially used by children use at least one tracking service, as opposed to 65% of the apps falling in other app categories". The authors showed that 19 popular and highly-ranked children games had even more than 10 third-party tracking and advertising domains, p. 6)

[13] See e.g. MijnkindOnline, How ONE stolen Twitter profile picture resulted in a worldwide smear campaign, available at: http://mijnkindonline.nl/artikelen/how-one-stolen-twitter-profile-picture-resulted-in-a-worldwide-smear-campaign. Tiziana Cantone: Suicide following years of humiliation online stuns Italy," BBC News, 16 September 2016. Jorg Leijten, "ROC hoeft niet mee te werken aan onderzoek seksfilmpje," NRC, 21 September 2016. Paul Farrel, "Nude photos of Jennifer Lawrence and others posted online by alleged hacker," The Guardian, 1 September 2014. Jayme Poisson, Teen facing charges for alleged online

harm and other stressful experiences. Such cases range from violations of data protection law, e.g. publication of photos without individual's consent, to other crimes closely related to personal data disclosure such as defamation, cyberharassment, cyberbullying, or online impersonation. Academic research confirms the occurrence of violations related to personal data misuse on an individual level listing the hacking of social media accounts, creation of fake profiles, and impersonation as actual situation that upset children online.[14]

The impact of commercial datafication and dataveillance on children cannot (yet) be fully envisioned today.[15] Equally, academics are still trying to map and understand the extent of harm arising from online risks posed by the interaction between individuals.[16] Nontheless, the explosive data-intensity and online collection undoubtedly contribute to the growth of online privacy risks, such as commercial exploitation and misuse of personal data, profiling, identity theft, the loss of reputation and discrimination. Therefore, it is no surprise that this has intensified debates and research about the impact of the described practices on children and their fundamental rights, especially the rights to privacy and personal data protection, among the general public, scholars, and policy makers.

The research with children suggests that children are not at ease online and feel that companies try to confuse them when collecting their personal data.[17] In addition, empirical studies show that privacy risks are common on the internet[18] and privacy concerns constitute one of the main worries among children in Europe.[19] In the same vein, adults widely support the introduction of special data protection measures for children. According to a Eurobarometer survey, 95% of Europeans believed that "under-age children should be specially protected from the collection and disclosure of personal data" and 96% thought that "minors should be warned of the consequences of collecting and disclosing personal data".[20]

Whereas at first, studies focused on gathering empirical evidence on online safety and online risks, with time, legal scholars became interested in the implications of these risks for privacy and data protection of children. Privacy and data protection as digital rights now feature prominently on the agenda of scholars studying digital risks to children, with some shifting from framing the research problem as protection from online risks to protection of digital rights.[21] There have emerged calls to transform children's rights, guaranteed by the UN

impersonation, 2 February 2012, available at: https://www.thestar.com/news/gta/2012/02/02/teen_facing_charges_for_alleged_online_impersonation.html

[14] Giovanna Mascheroni, Kjartan Ólafsson, *Net children go mobile: risks and opportunities*, 2 ed Educatt, 2014.

[15] Simone van der Hof, I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World, 34 Wis. Int'l L.J., 2016. D. Lupton and B. Williamson, The datafied child: The dataveillance of children and implications for their rights, 19(5) New Media & Society, 2017.

[16] Vera Slavtcheva-Petkova, Victoria Jane Nash & Monica Bulger, Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research, Information, Communication & Society Vol. 18 , Iss. 1, 2015.

[17] Coleman, S., Pothong, K., Perez, E. And Koene, A., Internet On Our Own Terms: How Children and Young People Deliberated About Their Digital Rights, 2017, available at: http://casma.wp.horizon.ac.uk/casma-projects/5rights-youth-juries/the-internet-on-our-own-terms/

[18] For example, according to the empirical data of the EU Kids online, 9% of children aged 11-16 in Europe have experienced personal data misuse online. See Sonia Livingstone et al., 'Risks and safety on the Internet: The perspective of European children' (LSE, EU Kids Online, London 2011).

[19] Giovanna Mascheroni and Kjartan Ólafsson, *Net children go mobile: risks and opportunities*, 2nd ed. Educatt, Milan 2014.

[20] European Commission, 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (June 2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> 196 and 203.

[21] Sonia Livingstone, Reframing media effects in terms of children's rights in the digital age, Journal of Children and Media, 10(1), 2016.

Convention on the Rights of the Child (UN CRC), to cater for the 'digital age'.[22] Among the rights to provision and participation, the UN CRC recognises children's rights to protection, including a specific protection against arbitrary or unlawful interference with children's privacy and unlawful attacks on their honour and reputation (Article 16).[23]

New theoretical concepts and frameworks in relation to children and their rights online emerged to consider the changing relationship between children, their rights and the digital dimension. The "datafied child" as a concept, developed by Lupton and Williamson, draws attention to the amount of data collected about children during their online presence and the impact of this collection on children's wellbeing and rights.[24] As a response to the various ethical and legal issues that the 'datafied child' raises, scholars have developed a children's digital rights research framework. This framework allows the exploration of digital media use by children through a rights-based approach and especially permits to balance children's need for protection with their capacity to maximize the opportunities online and, therefore, to "rethink (human and children's) rights and the digital". [25] In this context, academic efforts to reflect on particular child rights online through three conceptual lenses underpinning the UN CRC - protection, participation, and provision - started to emerge.[26] They clearly diverged from the traditional, predominantly protective stance towards children and added a significant emphasis on participation in the context of media and internet policy. This emphasis is in line with the focus on "autonomy and participation rights as the new norm in children's rights practice and policy" which, as demonstrated by Reynaert et al.,[27] is one of the main general research themes of child rights scholars since the adoption of the UN CRC.

Looking at the reaction of policy makers and the legislation, it becomes clear that only recently a child-specific perspective in the context of online privacy has been embraced.[28] For a long time, protection of online privacy in the EU has been designed for "everyone", conflating adults and children in one single group of data subjects. Since 1995, children are covered by

---

[22] Sonia Livingstone and Amanda Third, Children and young people's rights in the digital age: an emerging agenda, New Media & Society, 19(5), 2017; Sonia Livingstone and Brian O'Neill, Children's rights online: challenges, dilemmas and emerging directions in Simone van der Hof, Bibi van den Berg and Bart Schermer, (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Information technology and law series (24), Springer with T. M. C. Asser Press, The Hague, 2014.

[23] United Nations Convention on the Rights of the Child, 20 November 1989, 1577 UNTS 3 (UN CRC).

[24] Deborah Lupton and Ben Williamson, The datafied child: The dataveillance of children and implications for their rights **,** *New Media & Society*, 19(5), 2017.

[25] Sonia Livingstone, Amanda Third, Children and young people's rights in the digital age: An emerging agenda**,** *New Media & Society*, 19(5), 2017, p. 657.

[26] Simone van der Hof, I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World, 34 Wis. Int'l L.J. 409, 445 (2016). Eva Lievens, Children's rights and media: imperfect but inspirational, Eva Brems, Wouter Vandenhole and Ellen Desmet (eds.), Children's Rights Law in the Global Human Rights Landscape**:** Isolation, inspiration, integration?, Routledge, 2017. (Using the UN CRC as a framework, Simone van der Hof, analysed the regulation of children's consent as a mean of exercising children's rights to privacy and data protection in the EU and Eva Lievens discussed children's rights in information society.)

[27] Didier Reynaert, Maria Bouverne-de-Bie, Stijn Vandevelde, A Review of Children's Rights Literature Since the Adoption of the United Nations Convention on the Rights of the Child, *Childhood* 16(4), 2009, pp. 528-529.

[28] Council of Europe, Strategy for the Rights of the Child (2016-2021) (March 2016); UN Committee on the Rights of the Child, Report of the 2014 Day of General Discussion 'Digital media and children's rights', (May 2015); UNICEF, 'Privacy, protection of personal information and reputation rights' (2017) Discussion paper; UK Children's Commissioner, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (January 2017); UK House of Lords Committee on Communications, 'Growing up with the internet' (2nd Report of Session 2016–17) (March 2017), 2017.

the age-generic data protection provisions provided by Directive 95/46/EC[29] with no special focus on the processing of children's data. The newly adopted EU General Data Protection Regulation (2016/679)[30] (hereinafter - 'GDPR' or 'Regulation') has significantly changed the *status quo* and rejected the "age-blind" approach to data subjects. Only recently, the GDPR explicitly recognizes that children need more protection than adults and generates a child-tailored privacy protection regime, which aligns with other initiatives related to the protection of children's privacy online (codes of conduct, impact assessments).

This dissertation is an article-based research and started off several years ago in the midst of the developments sketched above. In a way, the articles presented in this dissertation testify to the rich academic debate in the domain of child-specific privacy protection and the impressive amount of insights that have been gained during the past few years. The articles written, submitted and published in the early period of this research are based on a body of literature that is far less rich than what is known and accepted at present. However, this also means that some findings of this research were published at a time when certain new academic insights, perspectives and protection models had not yet been presented. As a consequence, some of the earlier articles of this dissertation do not fully reflect all current academic perspectives and later articles entail some advancement in thinking on how specific legal provisions should be understood and interpreted (e.g. the GDPR provisions on profiling of children).

Although, within the now rich body of research the original contribution of the dissertation remains clear: the research combines social sciences and human rights law in considering privacy protection for children on the internet. Despite the large amount of available empirical data on privacy risks online, hardly any research has tried to translate empirical findings into the legal domain and apply the insights in the context of child's rights regimes. A key reason for the absence of such research appears to be the lack of appropriate expertise and methodologies or incentives from the outside world. In merging empirical research with legal/regulatory theories, this dissertation hopes to contribute to the academic debate on fundamental child rights as well as interdisciplinary research in the field of internet regulation. Although, some scholarly attention has been paid to the effectiveness of the emerging privacy protection regime,[31] neither its justification, nature and extent of the protections afforded to children's privacy online nor its implications to child rights, online behaviour and vulnerabilities have been examined in a combined effort of social sciences and (privacy) law. Based on desk research and empirical insights, this dissertation, therefore, hopes to contribute to a better understanding and justification of the necessity of specific regulatory privacy protection (through legal and soft-law tools) for children on the internet, to identify the existing gaps and unclarities, and consequently to consider how to improve the existing

---

[29] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281 , 23/11/1995, 31-50.*

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[31] A. Mantelero, Children online and the future EU data protection framework: empirical evidences and legal analysis. International Journal of Technology Policy and Law 2(2–4), 2016; J. Savirimuthu, Networked children, commercial profiling and the EU data protection reform agenda: in the child's best interests? In: Iusmen I and Stalford H (eds.) The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions. Opladen: Barbara Budrich Publishers, 2016, pp. 221–257; S. van Der Hof, No child's play – online data protection for children. In: Van Der Hof S, Van Den Berg B and Schermer B (eds) Minding Minors Wandering the Web: Regulating Online Child Safety. Information Technology & Law Series No. 24. The Hague: Springer Press/TMC Asser Press, 2014, pp. 127–141; Lina Jasmontaite and Paul de Hert, The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet, *International Data Privacy Law,* 5(1) 2015.

regulation. Given this, the overall aim of this dissertation is to investigate whether, and how, child-rights and social science perspectives can enrich the thinking about the specific regulatory regime adopted in the EU to protect children from privacy risks online and to improve the regulatory regime.

From a non-academic perspective, the dissertation intends to contribute to the broader societal, political and regulatory debate on the privacy risks for children and the role of regulatory measures in protecting them from these risks. Violations of privacy can result in long-term consequences, like stigmatisation and discrimination, and harm the social and emotional welfare of children. Future technological developments are likely to aggravate online privacy risks and harms. However, a predominantly protective perspective towards children taken by the regulators often fails to take into account the interests and experiences of children. An increased understanding of the risks and regulatory means to mitigate them, serves as a basis for protection of increasingly connected, ever younger children.

1.1. Background

Given the aim mentioned above, the dissertation revolves around three core notions. The first notion is the child. The dissertation uses a holistic and multidisciplinary understanding of this notion. It aims to view a child through two equally important lenses – legal and social – and to avoid considering a child only as a minor, a pure actor in law with his/her limited rights and responsibilities. As Lievens argues 'child' is a more general term, used in different contexts, the notion 'minor' is linked to the age of majority, and more often used in a 'legal' context".[32] By not limiting the notion of a child to a minor, the dissertation adds to the legal characteristics (competency and responsibility limitations and partial entitlements) an additional social science dimension - the needs and vulnerabilities, particular behaviour and perceptions of children as (still developing) social actors. It is also in line with the UN Convention on the Rights of the Child (UN CRC) terminology, which even if being a legal document, protects children's and not minors' rights.

The legal and policy debates presented in this dissertation unavoidably require the discussion about the age and age limits, as age from a legal perspective is a decisive boundary marker of the child concept. As will be shown in Chapter 3, appropriate age threshold fuelled the debate of parental consent in the GDPR. Although, important for lawyers, from the sociological childhood perspective age does not necessarily 'describe the lived experiences of children'.[33] Biological age is not a precise or uniform indication of physical, psychological and social development. Therefore, as noted by sociologists, "the mapping of an age- and stage-based categorisation schema onto children's social, intellectual and psychological development, irrespective of social context, is now regarded as problematic"[34]. Age has been considered a contested concept as it is used to define children and restrict, protect or allow their activities considering them as a group despite the differences among the children composing the group.

The dissertation refers to a child as an individual below the age of 18 years old, in line with Article 1 of the UN CRC. In this sense it uses the term 'child', an age-based construct, but acknowledges that other EU policy areas have considered 'child' to be a biological construct

[32] Eva Lievens, *Protecting Children in the Digital Era: the Use of Alternative Regulatory Initiatives*. Martinus Nijhof Online, Leiden, 2010, p. 29.
[33] Allison James, Adrian James, *Key Concepts in Childhood Studies.* Sage Publications Ltd, London, 2012, p. 1.
[34] Ibid.

or a dependency-based construct.[35] Despite the chosen definition, it should be clarified that theoretical and practical issues and the level of adequate protection are not identical for all children in this age spectrum.

The second core notion is regulation. Recognising that regulation as a concept is contested and subject to many different definitions in various fields of research, it requires clarification in this specific context. In this dissertation regulation has been assigned a wide meaning and the definition departs from the assumption that "anything producing effects on behaviour can be considered regulatory".[36] More precisely, as Scott defines it, regulation in this context is considered "any process or set of processes by which norms are established, the behavior of those subject to the norms monitored or fed back into the regime, and for which there are mechanisms for holding the behaviour of regulated actors within the acceptable limits of the regime"[37]. Regulation therefore includes different mechanisms of social control and embraces not only hard law but also soft law and other forms of social norms.[38] This wide view of regulation allows analysis of the chosen multifaceted EU regulatory model related to children's online privacy which entails hard law instruments (e.g. the GDPR, the Data Protection Directive 95/46/EC, Unfair Commercial Practise Directive, Consumer Rights Directive), soft law initiatives (e.g. the Safer Social Networking Principles, the CEO Coalition's Statement of Purpose, the ICT Coalition's Principles, and the FEDMA code) and self-enforced regulatory tools, such as data protection impact assessments (DPIAs).

As both protection of children online as a policy area and related empirical evidence have long been framed in terms of risks, the third core notion in this dissertation is risk. Notwithstanding the long-lasting academic debate on risk as a theoretical notion,[39] it should be acknowledged that there is no single definition of risk in general and privacy risk in particular. In the context of this dissertation, two often diverting perspectives on risk are considered: a sociological and a technico-scientific. As claimed in Chapter 5, European data protection law from its inception does not systematically follow one of the two understandings of risk and partially fits both technico-scientific and sociological perspectives. Therefore, this dissertation draws on: 1) the understanding of risk in social sciences, in particular the risk notion present in media and communication studies, the field from which the most empirical evidence on online risks for children emerged, and 2) the legal notion of risk, present in the EU risk regulation, GDPR and impact assessment frameworks. According to Staksrud, a scholar who studied online risks for children from the perspective of media studies, the most appropriate risk definition in terms of online risks to children is that of "possibility of loss or injury, or something that creates or suggests a hazard – a source of danger".[40] In addition to this general meaning of risk, media scholars acknowledge that risk is a constructed rather than a universally fixed notion. Individual perception of something as being a hazard is strongly shaped by various individual and collective factors, varying from socio-economic factors, regulatory framework, technological infrastructure to education system, or cultural values.[41] Particularly

---

[35] Helen Stalford, *Children and the European Union: Rights, Welfare and Accountability*. Hart Publishing, Oxford, 2012.

[36] Robert Baldwin, Colin Scott, and Christopher Hood, *A Reader on Regulation,* Oxford: Oxford University Press, 1998, p. 4.

[37] Colin Scott, Analysing Regulatory Space: Fragmented Resources and Institutional Design, Public Law, 2001, p. 331

[38] David Levi-Faur, Regulation and Regulatory governance, in David Levi-Faur (ed.) *Handbook on the Politics of Regulation*, Edward Elgar Publishing Limited, UK, 6.

[39] J. Frank Yates (ed.), Risk-taking behavior, Chichester: John Wiley, 1992.

[40] Elisabeth Staksrud, *Children in the Online World. Risk, Regulation, Rights*, Farnham: Ashgate, 2013.

[41] L Hasebrink, Uwe, Livingstone, Sonia and Haddon, Leslie, *Comparing children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online.* EU Kids Online, Deliverable D3.2. EU

relevant factors for understanding the online risks to children are social mediation of parents, school and peers, an individual usage of the internet.[42] Moreover, risks are often subjective constructs defined according to culture, ideology, norms, nationality, language or age.[43]
From a legal perspective, risk can be expressed as a negative impact on a data subject's rights and freedoms (the GDPR framing of risk) and as the probability that a vulnerability of an asset is exploited by a threat and negatively affects the confidentiality, integrity and availability of data and the impact of that effect (the data security-related framing of risk).[44]

1.2. Aim of the study and research question

As mentioned earlier, the aim of this dissertation is to investigate whether and how, child-rights and social science perspectives, can enrich the thinking about the specific regulatory regime adopted in the EU to protect children from privacy risks online and improve the regulatory regime. Clearly, it is not possible to systematise all potentially relevant aspects of this aim, within the ambit of a PhD. In the light of the developments described in the previous paragraph, the central research question to be addressed is:
How can EU law and self-regulatory initiatives protect children from online privacy risks while accounting for the particular characteristics of children?

Each part of this PhD dissertation contributes to answering this research question by focusing on four key dimensions, that in turn make up the four sub-questions:

- What are the characteristics that make the (online) position of children special and require a specific regime to protect them from privacy risks online in the EU?
- How has the child-specific online privacy protection regime thus far been constructed, i.e. what are the different levels, rules and tools employed in the EU?
- What are the dilemmas and unresolved challenges in terms of the particular characteristics and rights of children when implementing child-specific online privacy protection mechanisms in practice?
- What are the ways to improve the child-specific online privacy protection regime?

1. 3. Perspective of the study

1.3.1. The rights-based approach

The very title of this dissertation already suggests that this research should be clearly positioned in a 'rights' framework. Indeed, children are bearers of the rights to privacy and personal data protection under the international human rights instruments.[45] Human rights

---

Kids Online Network, London, UK, 2008; Elisabeth Staksrud, *Children in the Online World. Risk, Regulation, Rights*, Farnham: Ashgate, 2013, 53.

[42] Sonia Livingstone et al., Risks and safety on the Internet: The perspective of European children, LSE, EU Kids Online, London, 2011.

[43] Elisabeth Staksrud, *Children in the Online World. Risk, Regulation, Rights*, Farnham: Ashgate, 2013, 65

[44] ISO/IEC, "Information technology -- Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008 "*the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence".*

[45] Art. 16 UN Convention on the Rights of the Child, 20/11/89; Art. 12 Universal Declaration of Human Rights, 10/ 12/48; Art. 8 European Convention for Protection of Human Rights and Fundamental Freedoms, 04/11/50; Art. 24 EU Charter of Fundamental Rights, 07/12/00.

offer a compelling normative framework for the discussion of the child-related regulatory regimes in the EU.

The rights-based approach is at the heart of the UN CRC. Four principles distinguished by the Committee on the Rights of the Child are considered as horizontal when implementing and interpreting all the provisions of the UN CRC: non-discrimination (Art. 2), the best interests of the child (Art. 3); survival and development (Art. 6) and respect for the views of the child (Art. 12).[46] The UN CRC grants a comprehensive set of rights to children, which are commonly grouped into the rights related to protection, provision and participation.[47] This is the so called typology of "the three Ps" aims to describe the scope of the rights rather than segregate them into distinct categories. Such segregation "would be in breach of the comprehensive and holistic spirit of the CRC".[48] Therefore, as summarised by "the three *P*s have to be interpreted as *interdependent and indivisible* in the same way as the Convention itself: no protection without provisions and participation, no provisions without protection and participation, no participation without provisions and protection".[49] Although a shift in academic thinking – arguing against the grouping of the child rights in three categories or "three Ps"[50] – can be seen, this research opts to follow the traditional child rights approach in distinguishing protective, provisory and participatory rights. This approach might be challenged but is still broadly recognized and solid for the purpose of this research.

Acknowledging the interdependence and indivisibility of child rights, different perspectives underlying child rights law can still be employed as dominant in researching the position of children online and the protection they should be accorded. One can take the perspective of the right of a child to protection. Another perspective that could be applied is the child's right to emancipation (participation) and development. These perspectives become even more interesting portrayed as a dichotomy in practice, given that laws and regulations tend to opt for one of the other, implying both perspectives by default manifest a conflict. The combination of both would undoubtedly allow for a balanced approach in addressing challenges related to children, yet practical implementation of child rights might often lack this balance. As will be discussed in more detail in Chapter 2, the relationship between empowerment and protection elements can become a dilemma for legislators and therefore the chapter frames it as an "empowerment v protection" conflict. Also various authors – both media

---

[46] Committee on the Rights of the Child, General Comment No. 5 (2003) General measures of implementation of the Convention on the Rights of the Child (arts. 4, 42 and 44, para. 6), CRC/C/5, para. 13–14.

[47] Pia-Liisa Heiliö, Erja Lauronen, Marjatta Bardy (eds.), Politics of Childhood and Children at Risk, Provision, Protection, Participation, Eurosocial Report 45, Vienna, European Centre for Social Welfare Policy and Research.

[48] See also Committee on the Rights of the Child. CRC/C/58, 1996, Para. 9. General Comment No. 5 (2003), General measures of implementation of the Convention on the Rights of the Child. CRC/GC/2003/5.

[49] Eugeen Verhellen, The Convention on the Rights of the Child: reflections from a historical, social policy and educational perspective in Wouter Vandenhole, Ellen Desmet, Didier Reynaert, Sara Lembrechts (eds.) Routledge International Handbook of Children's Rights Studies, London, UK: Routledge, 2015, 50.

[50] For example, Reynaert et al., claim that the categorization of the child rights into the three Ps conceptualy weakens them, especially in comparison with general human rights law: 1) "it departs from the main categorisation human rights actors are familiar with, i.e. that of civil and political rights on the one hand, and economic, social and cultural rights on the other"; 2) the term 'provision rights', which refers to e.g. rights to education, health and social security, tends to confirm the outdated misunderstanding or misrepresentation that economic and social rights are exclusively about provision. It has meanwhile been widely accepted that the obligations relating to economic, social and cultural rights (ESC rights) are to be understood as obligations to respect, to protect and to fulfil, and that the latter obligation consists of sub- obligations to facilitate, to promote and to provide. Only the sub-obligation to fulfil-provide requires considerable mobilisation of resources." Didier Reynaert, Ellen Desmet, Sara Lembrechts and Wouter Vandenhole Introduction: A critical approach to children's rights, in Wouter Vandenhole, Ellen Desmet, Didier Reynaert, Sara Lembrechts (eds.) Routledge International Handbook of Children's Rights Studies, London, UK: Routledge, 2015, p. 7

scholars and child rights scholars – have explicitly referred to the tension between the two perspectives[51] and in their research preferred either agency or vulnerability as a paradigm.[52] As noted by Stoilova et al, "a rights framework is holistic, concerned with the full range of children's rights and, thereby, bringing into view the relation and potential conflict between protection and participation rights"[53]. Also, "a rights framework provides a normative lens through which to critically examine and evaluate the benefits or harms of children's growing access to and provision of digital technologies", for example avoid discussing "protection challenges without recognising how the resulting policy can curtail children's freedoms to participate online".[54] Yet, reliance on the rights-approach involves more than compatibility with the standards set forth in human rights law but rather widens the debate by allowing to reconceptualise children's role and questioning the responsibility of public and private actors in the regulatory context.

The rights-based approach has emerged in the area of international development[55] and only more recently this approach has also been adapted to the child-rights domain.[56] The heart of this approach is compose of a few core principles: participation, accountability, equality and non-discrimination, transparency, and empowerment.[57] Drawing on them, this approach provides the following benefits.[58]

First, the rights-based approach offers a useful child-empowering normative framework. The rights discourse itself already leads to the empowerment of children, and shifts the focus from their needs to their rights as legal entitlements. This is not the case when the risk discourse is employed and children are framed as vulnerable to risks from which they need to be protected. Such an approach imposes legal obligations on those who have to respect and implement the rights and conditions the prioritisation of different rights.

Second, the rights-based approach requires that both the regulatory outcome and the process achieved are in line with human rights.[59] For example, it draws attention to the active and informed participation by the right-holders in the formulation, implementation and monitoring of relevant policies and decisions. Such participation is desirable not just as a means to reach other ends, but as a fundamental human right in itself. In order to guarantee such participation, it requires to build specific mechanisms and arrangements at different levels of decision-making.

Third, the rights-based approach emphasises the responsibility of policy makers and other actors who have an impact on rights. It contributes to the increased accountability of

---

[51] Helen Stalford, *Children and the European Union: Rights, Welfare and Accountability*. Hart Publishing, Oxford, 2012. J. Fortin, *Children's Rights and the Developing Law*. Cambridge: Cambridge University Press, 2009. Mariya Stoilova, Livingstone, S. and Kardefelt-Winther, Global Kids Online: Researching children′s rights in a global digital age, *Global Studies of Childhood*, 6(4) 2016.

[52] See chapters by Gertrud Lenzer, Violence against children and by Kay Tisdall, Children and young people's participation, in Wouter Vandenhole, Ellen Desmet, Didier Reynaert, Sara Lembrechts (eds.) Routledge International Handbook of Children's Rights Studies, London, UK: Routledge, 2015.

[53] Mariya Stoilova, Livingstone, S. and Kardefelt-Winther, Global Kids Online: Researching children′s rights in a global digital age, *Global Studies of Childhood*, 6(4), 2016, p. 456.

[54] Ibid.

[55] Andrea Cornwall and Celestine Nyamu-Musembi, Putting the 'rights-based approach' to development into perspective, *Third World Quarterly* 25(8), 2004; Paul Gready, Rights-based approaches to development: what is the value-added?, *Development in Practice*, 18(6), 2008.

[56] Helen Stalford, *Children and the European Union: Rights, Welfare and Accountability*. Hart Publishing, Oxford, 2012.

[57] Paul Gready, Rights-based approaches to development: what is the value-added?, Development in Practice, 18(6), 2008.

[58] Adapted from HCHR *Principles and Guidelines* for a Human Rights Approach to *Poverty Reduction* Strategies. 2004.

[59] Helen Stalford, *Children and the European Union: Rights, Welfare and Accountability*. Hart Publishing, Oxford, 2012, 29.

states, EU institutions and other local authorities not only "in term of respecting and upholding human rights obligations, but also in terms of adapting or instituting processes that facilitate fulfilment of those rights"[60] Ferguson claims that framing the debate in terms of rights is in itself a "vehicle for increasing the accountability of government organisations to their citizens and consequently increasing the likelihood that policy measures will be implemented in practice".[61] Even more importantly, relying on the rights-based approach extends accountability for rights from states to private actors who are considered as duty bearers. The UN High Commissioner for Human Rights articulated this expanded notion of accountability as follows:

> *Perhaps the most important source of added value in the human rights approach is the emphasis it places on the accountability of policy-makers and other actors whose actions have an impact on the rights of people. Rights imply duties, and duties demand accountability.*[62]

Therefore, this approach allows "rendering the law real in political and social processes, as well as within the legal mainstream and through adherence to legal obligations", in other words, it makes human rights less declaratory and more operational.[63]

With this in mind, the dissertation explores to which extent the EU accounts for the substantial child rights and adheres to the processes and obligations inherent in the rights-based approach in regulating children's privacy protection online. It identifies the substantial provisions of the UN CRC that constitute the essence of the child rights-based approach[64] and explores how these rights are considered in the emerging EU child-specific privacy protection regime.

2. Theoretical framework

2.1. Social and institutional privacy

In line with the interdisciplinary perspective described above, this dissertation uses the distinction between social and institutional privacy as part of its theoretical framework. Social privacy is not widely known among lawyers. As a concept it is often used by social scientists

---

[60] Ibid.

[61] C. Ferguson, *Global Social Policy Principles: Human Rights and Social Justice*, London: DFID, 1999, p. 23.

[62] Cited in Paul Gready, Rights-based approaches to development: what is the value-added?, *Development in Practice*, 18(6), 2008, 735-747.

[63] Paul Gready, Rights-based approaches to development: what is the value-added?, *Development in Practice*, 2008 18(6), 736.

[64] Article 3: In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration. Article 13: The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice. Article 16: Protection of privacy. Children have the right to protection from interference with privacy, family, home and correspondence, and from libel or slander. Article 17: Access to appropriate information. The State shall ensure the accessibility to children of information and material from a diversity of sources, and it shall encourage the mass media to disseminate information, which is of social and cultural benefit to the child, and take steps to protect him or her from harmful material. Article 32: States Parties recognize the right of the child to be protected from economic exploitation and from performing any work that is likely to be hazardous or to interfere with the child's education, or to be harmful of the child's health or physical, mental, spiritual, moral or social development

to note "the ability to control the social situation by navigating complex contextual cues, technical affordances, and social dynamics"[65] in the networked publics. Social privacy, being about control of social situation and context (e.g. hiding from public environments), partially stems from Helen Nissenbaum's understanding of privacy through the lens of contextual integrity[66]. According to her view, privacy is defined by social context that based on its internal norms governs how personal information is disclosed and shared. Following this logic, privacy norms are "not once-and-for-all objective, but neither are they solely subjective", but "privacy is specified and co-constituted by means of the nature of the relationship we have with people, organisations, institutions, and even technologies".[67]

Social privacy refers to the negotiation of social boundaries, in particular to the management of diverse audiences through privacy settings and controls, and is entangled with online safety. This theoretical framework therefore allows include into the study peer to peer privacy risks and concerns online which are the result of data flows disrespecting social boundaries and contexts (undesirable contacts, damaged reputation, stalking, impersonation). Such concerns are alternatively difficult to capture from a purely legal regulatory perspective. For example, EU data protection laws excludes the processing of personal data by a natural person in the course of a purely personal or household activity from its scope.

Social privacy significantly differs from institutional privacy, which is more closely aligned with the aims of personal data protection law to safeguard individuals from illegal and illegitimate data collection and use by state institutions and private companies. Institutional privacy refers to the control of the flow of personal data. It emerges from the understanding of privacy proposed by Westin,[68] who defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[69] It does not emphasise the importance of the context in which data disclosure and processing takes place and its collision, but provides data controller-centric requirements. Although starting from different assumptions and often explored using different research methods, both privacy perspectives are entangled and can complement each other.[70]

2.3. Sociological perspective on childhood

The dissertation is grounded in the new sociological perspective of childhood, which became prominent after the 1990s. Social scientists following this perspective look at children as social actors for its own sake and not as 'incomplete' or 'in process' future adults.[71] Children are recognised as being 'capable of making sense of and affecting their societies'[72]. Thus, this perspective provides competence to children to "interpret the social word and act on

[65] danah boyd, *It's Complicated: the Social Lives of Networked Teens*, New Haven, CT: Yale University Press, 2014, p. 60.
[66] Helen Nissenbaum, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Palo Alto: Stanford University Press, 2010.
[67] Andrew McStay, *Privacy and the Media*, Sage Publications Ltd, 2017, p. 162.
[68] Alan F Westin, *Privacy and Freedom*. New York: Athenum, 1967.
[69] Ibid., 7
[70] Seda Gürses and Claudia Diaz, Two tales of privacy in online social networks, *IEEE Security & Privacy*, Vol. 11, 2013.
[71] Allison James and Alan Prout (eds.) *Constructing and Reconstructing Childhood: Contemporary Issues in the Sociological Study of Childhood*. London: Falmer, 1997. For an overview see S. H Matthews, A window on the 'new' sociology of childhood. *Sociology Compass*, 1(1), 2007.
[72] S. H Matthews, A window on the 'new' sociology of childhood. *Sociology Compass*, 1(1) 2007.

it".[73] Scholars following the new sociology of childhood advocate directly taking children's views into account instead of listening to adults perspectives over children's matters.

This perspective also elucidates the fact that children are not a homogeneous group and various factors contribute to different childhood(s) or 'the plurality of childhoods' lived by children.[74] Thus, as summarised by Matthews, "(a)ny statement that claims to describe children must deal with the question, 'Which children and under what circumstances?'"[75] It is recognised that "the everyday lives of children are experienced through social relationships with other children but perhaps more significantly with adults who control institutions that justify and support the type of dependency that children experience".[76] In the context of the present research, it allows to avoid falling into the trap of attaching to children generic labels such as 'digital natives' or 'millennials', overlook their diversity and ignore developmental characteristics or specific age-related needs. It also helps in advocating the age-specific data protection requirements in both law and self-regulatory instruments.

According to the sociological perspective on childhood, children are viewed as beings rather than beings in the making, refusing both biological reductionism and age-based determinism. In the context of this dissertation, the sociological perspective on childhood provides a lens to view children as agents and right-holders whose voices and perspectives should be accounted in research and law. In viewing children as collaborators and actors[77] rather than research objects (by gathering research data directly from children), this research intends to facilitate the discovery of new insights that can inform policy and practice on children at national, regional and global levels. Regarding children as actors also recognizes their role in the dynamic interplay of multiple processes, interests and actors that ultimately shape the way technology is being used.[78] Children can be considered to play such a role, given their interests are taken into account in democratic processes, among them the legislative provisions discussed in this dissertation that aim to protect their specific interests.

3. Methodology

The diverse research questions raised in this dissertation require different research methods to be employed in order to answer them. Descriptive questions addressed in Chapter 2 and partially in Chapters 3, 4 (*what/how is the child privacy protection regime constructed?, how does this regime compare with other legal regimes?)* and Chapter 7 (*how do self-regulatory instruments compare among them?*) to a great extent call for a doctrinal research method. An explanatory question (*why is this legal regime needed?)* raised in Chapter 3 and a more design-oriented question: (*how can the regime be improved?*) tackled in Chapters 5 and 6 predominantly require external insights from other academic fields. As a result, the dissertation embraces "methodological pluralism"[79] and combines traditional doctrinal research with interdisciplinary research through insights and data from other disciplines.

---

[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] An actor is something or someone who makes a *difference* in a relationship. B Latour, *Reassembling the Social. An Introduction to Actor-network-theory*, Oxford, Oxford University Press 2005.
[78] W Bijker and J Law (eds.), *Shaping Technology/Building Society. Studies in Sociotechnical Change*, Cambridge, MA, MIT Press, 1992.
[79] Christopher McCrudden, Legal Research and the Social Sciences. Law Quarterly Review. 122, 2006, 532-650. (McCrudden refers to the methodological pluralism when doctrinal legal analysis supports or tests their doctrinal or theoretical models by drawing on social science influenced information.)

3.1. Doctrinal research

Doctrinal or legal-dogmatic[80] research can be defined as "research that aims to give a systematic exposition of the principles, rules and concepts governing a particular legal field or institution and analyses the relationship between these principles, rules and concepts with a view to solving unclarities and gaps in the existing law"[81]. In the context of this dissertation, a critical conceptual analysis of the legal sources relevant to the protection of children's online privacy has been performed in order to expose the current state of the law and the existing discrepancies, ambiguities and challenges. The protection of children's online privacy has been viewed as a single, multi-layered system, in which elements of national, European and international law, hard and soft law form a whole. The primary sources of analysis include relevant international law (UN Convention on the Rights of the Child, the European Convention on Human Rights), European law (the of Fundamental Rights of the EU, GDPR, Directive 95/46/EC) and national rules (e.g., national data protection laws), opinions and comments issued by the UN Committee on the Rights of the Child, Article 29 Working Party and national data protection authorities, available case law and legal literature. Where appropriate, references were made to preparatory works and policy discussions of the GDPR to gather additional insights to those offered by the primary sources.

3.1.1. Comparative analysis

Several articles in this dissertation include comparative analysis which is both external and internal in its nature. External comparative legal research is used to compare legal concepts and provisions adopted to protect children's privacy online among different legal jurisdictions and legal families. Chapter 3 compares the rules on the consent of minors to their personal data processing in two different legal orders (i.e. the US (COPPA) and the EU (GDPR)) in order to reveal similarities and differences and provide suggestions for the improvement of the GDPR. The same chapter also looks into the national data protection laws of the EU Member States to compare existing provisions on the role and capacity of children as regards their personal data processing.

An internal comparative analysis, focusing on the comparison of legal concepts and principles of different fields of law (consumer and data protection law) in the EU legal system, is carried out in Chapter 4. The method of internal comparative analysis proposed by Vranken looks for intersections, crosslinks and commonalities between different fields of law.[82] Although each legal field has its own principles, instruments and sanctions, the various areas should be treated alike in order to maintain coherence of the legal system as a whole.[83] This method is particularly appropriate to appreciate the differentiated roots of specialised areas of law as well as to coherently apply the same human rights standards to different areas.[84] In fact,

---

[80] J.B.M. Vranken, 'Exciting Times for Legal Scholarship', *Recht & Methode in onderzoek en onderwijs* 2012, 42

[81] Smits, Jan M., What is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research, September 1, 2015. Rob van Gestel, Hans-W. Micklitz & Edward L. Rubin (eds.), Rethinking Legal Scholarship: A Transatlantic Dialogue, New York, Cambridge University Press, 2017, pp. 207-228.

[82] J. B. M. Vranken, Interne rechtsvergelijking, Tijdschrift voor privaatrecht, 1995, available at: https://pure.uvt.nl/ws/files/369319/TPR95.PDF

[83] Ibid.

[84] Ibid.

cross-links and mutual influence between consumer law, contract law and data protection law are strong and it is difficult to imagine their interpretation without their comparison and (at least partial) integration. Chapter 4 therefore aims to draw from consumer law notions and principles, such as transparency and fairness, in order to extend the less robust constructs of the child currently seen in the GDPR as well as to enhance the level of protection for children acting as both data subjects and consumers online.

3.2. Interdisciplinary research

Although doctrinal legal analysis is essential to examine and understand the law as it stands, it follows an internal approach and mainly focuses on textual analysis of laws and judicial reasoning.[85] Being concerned with how to improve the current legal system in terms of coherence and consistency, doctrinal research does not allow for the simple integration of external perspectives or data outside of current positive law.[86] As a result, the doctrinal approach alone is able "to provide only partial representations of the complicated interplay between law and society in the field of child online privacy".[87] Indeed, it would be impossible to answer the main research question (to propose the improvements for the child-specific regulatory regime) without knowing if this regime accounts for children's lived experiences and needs. Therefore, the legal rules of the regime under study should be viewed and interpreted in their proper social context and with an understanding of the individuals to which they relate[88]. As a consequence, legal analysis needs to be put into dialogue not only with child rights scholarship but also with social science findings about children's experiences as both data subjects and socio-technical agents in their own rights. In other word, insights into the online behaviour, privacy perceptions and special interest and vulnerabilities of children and adolescents are essential additional knowledge which should be taken into account if one aims to understand the current regulation and its possibility to achieve protection and provide proposals for improvement. This requires an external perspective on the law. Therefore, the insights from non-legal disciplines are intentionally applied to varying extents in all the chapters of the dissertation. Such social science findings emerge from empirical studies on how

---

[85] It should be recognised that doctrinal or legal-dogmatic research is not a uniform concept. As noted by Vranken, "(p)erspectives, approaches, or methods that might seem relevant to some, others regard as conflicting with legal-dogmatic research or even as non-legal. For example, the search for 'better' solutions to a problem, a common issue in legal-dogmatic research, is usually not aimed at a better legal-technical foundation but rather at a substantive legal contribution to better fulfil the requirements of society. However, such questions cannot be answered from a strictly internal dogmatic perspective. Those arguing for more open reasoning also use knowledge and viewpoints that others regard as falling outside the scope of legal dogmatism. The development that private law has seen over, say, the last thirty-five years would have been impossible if legal-dogmatic research had always kept to the limits of an internal perspective and 'the' system." J.B.M. Vranken, 'Exciting Times for Legal Scholarship', *Recht & Methode in onderzoek en onderwijs,* 2012, 42.

[86] According to Vranken, consistency and coherence of the legal system are important but not the only possible and desirable perspectives for legal doctrinal research. Vranken claims that more perspectives can be used by legal researchers conducting legal doctrinal research and questions, "why should a consistent and coherent system be preferable over, for example, social justice, improving the wellbeing of people, the proper functioning of markets, practicality, functionality, effective- ness or europeanisation and globalisation?".

[87] Alessandro Mantelero, Children online and the future EU data protection framework. Empirical evidences and legal analysis. International Jour. Tech. Policy & Law, 2016 (2/3/4): 169-181

[88] Vranken states: "The law does not exist in a vacuum: it attempts to regulate and influence human behaviour and social developments. Therefore, it is quite obvious that creating a proper legal system requires knowledge of what motivates people and of the social situation in which they function." J.B.M. Vranken, 'Exciting Times for Legal Scholarship', *Recht & Methode in onderzoek en onderwijs* 2012, 52.

children use new digital, networked and mobile technologies from the EU Kids Online, Net Children Go Mobile, Young Canadians in a Wired World, and Global Kids Online projects. The latest national empirical studies conducted in several EU countries, such as by Steijn in the Netherlands[89], by Mantelero in Italy[90]and by OFCOM in the UK[91] are also drawn upon. The social sciences provide especially useful evidence for criticising the existing provisions and making recommendations for their improvement.

However, the dominant perspective of the research remains legal. Indeed, although insights from the social sciences are necessary to answer the research question and to define the research problem, these do not transgress the boundaries of law but rather provides external input and factual knowledge for the development and improvement of the existing system (social sciences are used as auxiliary discipline).[92] Such an extension of the boundaries into the social sciences is in line with the theoretical lenses of the study (the social construction of privacy and the sociological understanding of childhood) which contribute to a richer understanding of the complexities of translating regulatory frameworks into practice. It also mitigates against simplistic or deterministic arguments about the role of technology in children's lives.

An even broader interdisciplinary perspective is visible in Chapter 5 and Chapter 6, incorporating the broad insights not only from social sciences but also from other external approaches (computer science and regulation and governance studies). When dealing with risk conceptualisation and assessment Chapter 5 builds explicitly on the external perspective of information security (i.e. computer science) and risks regulation. Chapter 6, as it was co-authored with the computer scientists, extends reliance on external non-legal disciplines even further as it uses a risk assessment methodology stemming from the information security domain to conduct a legal assessment of the possible impact on data subjects' rights. The framework proposed in Chapter 6 combines law, computer science also social sciences insights in order to account for a multidimentional concept of risk. This way of bringing disparate perspectives together allows for the discussion of risk to go beyond the typical approach to data protection impact assessments and thus the insertion of an understanding of risk as a socio-cultural construction that is implicated in the everyday lives of children. At the same time this permits one to challenge technical understandings of risk which use measurable proxies and flatten the rich social experience of privacy.

3.3. Data gathering

Two main ways of data gathering have been used: desk research and a survey conducted by the author. In order to further acquire necessary national (often publicly unavailable) legal sources and data, the national practices of EU Member States in the area of children's online privacy (national laws, case law and decisions of the national data protection authorities) have been explored based on a questionnaire submitted to the national data protection authorities (DPAs) in all 28 EU Member States. The questionnaire contained five open questions on: 1)

---

89 Wouter Steijn, Developing a sense of privacy, Phd dissertation, Tilburg university, 2014, available at: https://pure.uvt.nl/ws/files/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf

90 Alessandro Mantelero, Children online and the future EU data protection framework. Empirical evidences and legal analysis. International Jour. Tech. Policy & Law, (2/3/4) 2016.

91 OFCOM, Children and parents: media use and attitudes report, November 2016, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

92 Sanne Taekema and Bart van Klink, On the Border. Limits and Possibilities of Interdisciplinary Research, in: B.M.J. van Klink and H.S. Taekema (eds.), Law and Method. Interdisciplinary Research into Law, Tübingen: Mohr Siebeck 2011.

specific legal provisions regulating the protection of children's (age below 18) personal data online; 2) complaints related to the infringement of children's privacy/data protection rights online; 3) court decisions relating to the infringement of children's privacy/data protection rights online; 4) soft law instruments (codes of conduct, guidelines, principles, etc.) adopted on the national level aiming to protect children's personal data online; 5) any other relevant information (documents, reports, surveys, etc.) in light of the research topic. 29 DPAs from 25 EU Member States responded to the survey. Czech Republic, Ireland and Malta did not provide their responses, and 4 German state DPAs (from Baden-Württemberg, Brandenburg, Mecklenburg-Vorpommern, Rheinland-Pfalz) responded to the survey. A full overview of the questions and answers is available in Annex 1.

The main findings of the survey can be summarised as follows. First, there is a lack of specific national provisions on children's privacy and data protection. Only 5 DPAs (Hungary, the Netherlands, Spain, UK (for Scotland) and Italy) indicated the existence of such provisions. In Hungary, the Netherlands and Spain child-specific legal provisions relate to the age and other requirements for consent and in Scotland to the right of access to personal data. In Italy, specific safeguards are provided against the dissemination (including online) of information related to children involved in judicial proceedings and in the journalistic field (the child's right to privacy takes precedence over both freedom of expression and freedom of the press). The lack of specific provisions for children as data subjects is not compensated by DPAs themselves, as only the Belgian DPA has issued a formal recommendation on the subject. Latvian and Dutch DPAs addressed the topic in broader guidelines when discussing respectively the school and online data processing contexts. Other DPAs tackled the issue by occasionally issuing leaflets (Bulgaria, Slovenia), writing articles and opinions (France, Slovenia) and carrying out studies (Hungary, Poland). A number of DPAs have been involved in active, long-term awareness raising activities, e.g. created dedicated websites (Spain, UK, Portugal, the Netherlands, France, Belgium) to provide information and guidance to children, parents and educators and carried out trainings (Greece, Brandenburg). Although the national data protection laws generally cover minors to the same extent as adults, that lack of specific legal provisions and official guidelines from the DPAs leads to a situation where it is difficult to know how the data protection requirements need to be interpreted in relation to children. Many questions remain directly unanswered on a national level, e.g. from which age can a child give a valid consent, when and how can the child exercise his data subject rights and can he or she alone lodge a complaint with a data protection authority if his or her personal data processing infringes the law. Also, it is not clear if the exercise of data subject rights relates to the age limit from which the child can consent for his/her data processing and indeed if it should relate. Furthermore, the DPAs are focused on protection and are not inclined to place the discussion into the broader child rights or UN CRC context and note possible tensions between child rights and principles. Awareness raising is often framed in terms of risks rather than benefits and empowerment online. Only the Belgian DPA clearly underlines its aim to educate children and young people about the importance of privacy and responsible behaviour online without stressing dangers but rather possibilities, and reconciling young people's privacy with the positive impact of modern technologies.

Second, despite the fact that many DPAs do not have specific statistics on complaints submitted by children or their representatives, such complaints in the period of 2009-2014 were considered rare. 7 DPAs have received no complaints at all and many DPAs mentioned just a few complaints that had been lodged. Often complaints related to the publishing of children's data or photos online by schools, newspapers or social media users. The number of complaints might depend on the functions of the DPAs as not all of them are responsible for the supervision of data processing in media and journalistic activities. For example, the Italian DPA has such a function and had reported many cases of unlawful publication of children's data in the

journalistic context, while Lithuania reported no complaints indicating that the supervision of children's personal data processing in media falls under the responsibility of the Office of the Inspector of Journalist Ethics. The case also might be that children are more inclined to raise their concerns directly with the data controllers, e.g. report violations though the special report buttons or initiate erasure requests online. The low number of complaints, however, might also be an indication of the barriers to the availability and effectiveness of access to justice for children in the area of data protection across Member States. Even when a child is sufficiently able to identify and articulate a violation of his or her privacy and step forward to lodge a complaint with a data protection authority, many constraints may come into play, such as legal representation or legal knowledge. In fact, "(c)hildren's special status places them in a difficult position for pursuing remedies when breaches of their rights occur, because of lack of knowledge, ability and independence".[93] Therefore, as claimed by the Committee on the Rights of the Child, "(…) states need to give particular attention to ensuring that there are effective, child-sensitive procedures available to children and their representatives", such as the provision of child-friendly information, advice, access to independent complaints procedures with necessary assistance.[94]

Third, the majority of the DPAs could not provide information on relevant court decisions. This does not necessarily mean that such decision do not exist, but rather probably shows that the DPAs have troubles in getting an overview of the relevant court work. Some DPAs explicitly mentioned that none of their decisions have been challenged in courts and could not report about the other cases which were brought by individuals directly to the courts on data protection matters.

Fourth, there is a wide divergence in educational initiatives carried out by the DPAs. Many of the DPAs are engaged in or carry out awareness raising and educational activities related to children's personal data. Some of them are particularly creative and innovative, such as the "youth to youth" discussion model implemented by the CNIL. However, 13 DPAs did not explicitly mention their involvement in awareness raising. One DPA even claimed that parents and children have enough information on protection online.

It is important to note that the survey was distributed in June 2014, and since then many national legislators, DPAs and other authorities have been faced with questions on the age of consent due to the need to implement Article 8 of the GDPR. It is possible that more clarity and guidance has emerged on the subject than the responses document, more court decisions have been adopted and more new initiatives have been initiated. Also, there have been several important amendments in the national data protection laws, e.g. in France (on the right to erasure)[95] and Italy (on cyberbullying)[96], which are not reflected in the survey results.

4. Structure of the argument

This dissertation is composed of six separate articles that have been published or accepted for publication in refereed academic journals and a concluding chapter. Together these chapters reveal the limitations and possible improvements of the emerging multi-layered

[93] Beqiraj and L McNamara, Children and Access to Justice: National Practices, International Challenges (Bingham Centre for the Rule of Law Report 02/2016), International Bar Association, October 2016, p. 20.

[94] CRC, General Comment No 5, General Measures of Implementation of the Convention on the Rights of the Child, 27 November 2003, para 24.

[95] Article 40 and 58 of the French Data Protection Act of 1978.

[96] Anti-bullying law (Legge 29 maggio 2017 n. 71).

European regulatory regime aiming to protect children from online privacy risks separately from adults.

Each distinct publication focuses on a selected dimension of this new regulatory regime. These selected dimensions present the topical issues within the child online privacy protection debate, including the questions of: justification of the child-specific privacy regime, online privacy risk conceptualisation and assessment; limitations and gaps of the EU legislation (especially the General Data Protection Regulation) and self-regulatory child privacy protection schemes.

The first publication (Chapter 2), "From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation" presents the new child-tailored online privacy protection provisions in the EU General Data Protection Regulation (GDPR) and explores the dilemmas that the introduction of such provisions creates – the 'empowerment versus protection' and the 'individualized versus average child' dilemmas. It concludes that by favouring protection over the empowerment of children, the Regulation risks limiting children in their online opportunities, and by relying on the average child criteria, it fails to consider the some of the cornerstone elements of the UN CRC, namely evolving capacities and best interests of the child.

The second publication (Chapter 3) "Consent for processing children's personal data in the EU: following in US footsteps?" zooms in on the core child protection provision and the most controversial regulatory issue in the EU – the GDPR parental consent requirement. The GDPR requires parental consent before information society service providers can process the personal data of children under 16 years of age (unless national laws state otherwise). Being new this provision faces many interpretation and implementation challenges in Europe, but not in the US, which adopted detailed rules for the operators that collect personal information from children under the Children's Online Privacy Protection Act (COPPA) almost two decades ago. The article critically assesses the GDPR parental consent requirement, and makes a comparative analysis with the rules stipulated in the COPPA in order to identify pitfalls and lessons to be learnt.

The third publication (Chapter 4) "Protecting children as data subjects online: combining the rationale and rules of personal data and consumer protection law" reflects on the double role that children play online where they are not only data subjects but also consumers, and explores the extent to which EU consumer law, which takes account of children as a particularly vulnerable group of consumers for a long time, can inform the newly adopted General Data Protection Regulation. The analysis focuses on the reasons justifying the child-specific protection regime, principles (fairness, transparency) in relation to children, and conceptual questions (definition of an average child and services directed to children).

The fourth publication (Chapter 5) "The "riskification" of European data protection law through a two-fold shift" explores how risk is conceptualised and assessed in the General Data Protection Regulation. It claims that the role and meaning of risk can be understood through two distinct shifts: towards risk-based regulation and towards risk regulation of data protection law. The paper concludes by outlining some unresolved challenges stemming from the two shifts. This chapter constitutes an introductory part to the further analysis of online privacy risk assessments in the context of the GDPR.

The fifth publication (Chapter 6) "Constructing Child Specific Privacy Impact Assessments" builds on the previous chapter and further explores how more specifically privacy risks for children as data subjects can be defined and assessed using the data protection impact assessments. It adapts the general GDPR requirements for the DPIA to cases when data subjects are children and illustrates how a child-specific DPIA could be carried out based on the PRIAM methodology.

The sixth publication (Chapter 7) "Protecting Children's Privacy Online: A Critical Look to Four European Self-regulatory Initiatives" looks beyond data protection and consumer protection law and focusses on an alternative approach to regulation – self-regulation. The article examines the rise of self-regulatory initiatives as private governance mechanisms adopted by the Internet industry in the EU to protect children's privacy online. It analyses four specific initiatives and performs a formal self-regulatory process analysis focusing on procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors) aspects, in order to reflect on the strengths and shortcomings of the self-regulatory process. The analysis shows significant limitations of self-regulation in the area of online child safety, characterized by broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often inexistent sanctions. It is argued that sector-specific, institutionalized European codes of conduct, which disentangle protection of online safety and privacy as policy aims, could permit achieving better formulation, adoption and enforcement of voluntary rules, and thus better safeguard the privacy of children in the dynamic multi-jurisdictional, multi-stakeholder dominated online environment.

The final chapter (Chapter 8) serves as the conclusion to this PhD dissertation. It builds upon the joint publications and provides a final contribution to answering the central research question. Drawing upon the main evidence from empirical and legal perspectives it shows how the existing regulatory regimes relate to online behaviour, vulnerabilities and the rights and freedoms of children, i.e. the particular characteristics of children. The chapter provides suggestions on how the emerging child-tailored online privacy protection regime can be fine-tuned and improved.

Chapter 2

From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation

Published in a peer-reviewed journal as:

Macenaite M., From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation, 19(5) New Media & Society, 2017, pp. 765 – 779.

Abstract

The new European Union (EU) General Data Protection Regulation aims to adapt children's right to privacy to the 'digital age'. It explicitly recognizes that children deserve specific protection of their personal data, and introduces additional rights and safeguards for children. This article explores the dilemmas that the introduction of the child-tailored online privacy protection regime creates – the 'empowerment versus protection' and the 'individualized versus average child' dilemmas. It concludes that by favouring protection over the empowerment of children, the Regulation risks limiting children in their online opportunities, and by relying on the average child criteria, it fails to consider the evolving capacities and best interests of the child.

Keywords

Children, data protection, EU, General Data Protection Regulation, online privacy

1. Introduction

Children, who are increasingly becoming active Internet users at an ever-younger age, are either intentionally providing or unconsciously 'bleeding' increasing amounts of their personal data online. This growing intensity in providing personal data is seen as enhancing online privacy risks, such as the loss of reputation, commercial exploitation of personal data, profiling, identity theft, cyber harassment and discrimination. Given these risks, there have been increasing calls among policy makers and academics to provide exceptional treatment for children online, that is, to transform children's rights to privacy (established in Article 16 of the United Nations (UN) Convention on the Rights of the Child, UN CRC) for the 'digital age' (UN, 1989).

The most recent example of how such calls have been translated into practice in Europe is the General Data Protection Regulation (2016/679) (hereafter 'Regulation'), the main personal data protection legislation recently adopted in the European Union (EU).[1] The Regulation updates the Data Protection Directive (95/46/EC) and aims to strengthen citizens' fundamental rights, especially the right to privacy and personal data protection, in the digital age. At the same time, it allows for free data flows in the Digital Single Market by simplifying rules for

companies. It establishes, among other requirements, general data protection principles and legal grounds for data processing, and imposes various duties on entities processing, or deciding how to process, personal data (data controllers). The Regulation also provides individuals whose data is processed (data subjects) with certain rights, such as the right of access to their personal data, rights to data correction and erasure.

The Regulation, in contrast to its predecessor, explicitly recognizes that children deserve their personal data to be specifically protected, 'as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data' (Recital 38). It introduces far-reaching changes in relation to the processing of children's personal data: it requires prior parental consent before the processing of children's personal data and foresees other additional rights and safeguards.

Although much scholarly attention has been paid to the effectiveness of the new data protection framework, the Regulation has rarely been examined in relation to the nature and extent of the protections afforded to children's personal data online (Jasmontaite and De Hert, 2014; Mantelero, 2016; Savirimuthu, 2016; Van Der Hof, 2014). This article, therefore, explores the way in which the Regulation responds to the 'empowerment versus protection' dilemma in relation to children, that is, empowers children as Internet users able to grasp the opportunities of playing, learning and communicating, while protecting them from privacy violations and harm. It also explores the extent to which the individual understanding and development of each child is taken into consideration by the Regulation when balancing child rights against the powers and responsibilities of the parents ('individualized vs average child' dilemma).

The article begins with a brief description of the two dilemmas, both of which are intrinsically present in child rights law, created by the adoption of the child-specific online privacy protection regime. It then analyses how the EU legislator addressed these dilemmas and foresees future challenges.

2. Two old dilemmas in child rights law

The 'empowerment vs protection' dilemma is not new to child rights debates, but is, rather, part of a larger fundamental conflict underlying the whole of child rights law. This conflict is intrinsic to the UN CRC, due to the potential tensions between articles pertaining to protective rights and those pertaining to participatory (emancipatory) rights. Children's protective rights, such as the right to protection from ill treatment and abuse, as well as the right to state intervention in order to guarantee said protection, stem from their vulnerability, dependence on adults and need for physical and psychological care and nurture. Participatory (emancipatory) rights include children's claims to 'decision-making rights' (Fortin, 2009: 17), and are close to adult human rights, such as the right to freedom of expression and thought. The dilemma also relates to the tensions among several principles on which the UN CRC is built, such as the best interests of the child and the evolving capacities, participation and self-determination of the child. Efforts to support the best interests of children require participation from children, but there is an inherent contradiction between the two children's roles as 'beneficiaries of intervention by adults' and 'competent social agents in their own right' (Boyden and Levison, 2000: 52). The dilemma, therefore, can be seen as being 'one of the most fundamental challenges posed by the Convention on the Rights of the Child' (Lansdown, 2005: 32).

The same 'empowerment versus protection' dilemma has been partially embraced by Article 24 of the EU Charter of Fundamental Rights. As McGlynn (2002) frames it, 'Article 24(1) is a curious mix of what might loosely be termed children's "protection" and "empowerment" rights, which are often found to be in conflict' (p. 397). The Charter explicitly echoes the tension between the child's right to express his or her views freely, which should be taken into consideration in accordance with a child's age and maturity, and the right to protection, when decisions are taken on behalf of the child, in his or her best interests.

In his seminal article on children's rights, Eekelaar (1986) identified three categories of interests that children may claim: basic (physical, emotional and intellectual care), developmental (equal possibilities to maximize available resources) and autonomy (freedom to choose their lifestyle and to enter into social relations). These interests potentially interact: the developmental interests can be advanced if autonomy is exercised, even if mistakes are made, because a child can learn from them (Gilmore and Glennon, 2014). However, the different interests can also conflict, especially in cases when an adolescent's exercising of their autonomy conflicts with their basic interests (e.g. physical wellbeing). A false dichotomy also exists between the protection of children and the protection of their interests (Freeman, 1993). Freeman (1993) points out how

> [c]hildren who are not protected, whose welfare is not advanced, will not be able to exercise self-determination: on the other hand, a failure to recognize the personality of children is likely to result in an undermining of their protection with children reduced to objects of intervention. (p. 42)

Although the age and maturity (physical, emotional, cognitive and social development) of the child should guide the balancing of the protection and empowerment elements when balanced against each other, that is, help to solve the aforementioned 'empowerment versus protection' dilemma, it is difficult to assess when an individual child is competent to take responsibility for a decision affecting him or her. This is the second 'individualized versus average child' dilemma discussed in this article.

The challenge underlying the 'individualized versus average child' dilemma of determining the age at which specific protection for children should be lowered, taking into account the individual understanding and development of each child, is well illustrated by Lansdown (2005):

> It is not possible to prescribe defined ages at which all children need greater or lesser protection or opportunities for assuming responsibility. Nor is it possible to create sufficiently flexible legal and social frameworks through which to accommodate the widely varying capacities of children over different aspects of their lives. The former flies in the face of the evidence about how children's capacities evolve. The latter risks exposing children to exploitation and abuse. (p. xiv)

Efforts to draw a line, whereby the age demarcating the full legal capacity of children is determined, are often artificial and arbitrary when seeking, in the words of anthropologist Mary Douglas (2013), 'to satisfy social demands for clarity, which compete with logical demands for consistency' (p. 113). But from a legal perspective, the legislature may favour the application of a bright-line rule based on age, that is, a clearly set standard leaving no room for the exercise of discretion and assessment of an individual situation. As noted by the European

Court of Human Rights (ECHR, 2006), bright-line rules can help 'to produce legal certainty and to maintain public confidence in the law in a highly sensitive field'. They are also easy to apply and eliminate possible arbitrariness and bias (Federle, 2013). A case-by-case assessment of the individual's abilities is, administratively, excessively burdensome, particularly in the online environment. In addition, as noted by Scarre (1980), 'once set, the boundary introduces a quantitative distinction between adults and children, which treats (or has treated) everyone equally, namely the amount of time allocated to acquire experience before adulthood' (p. 117). However, as bright-line rules are absolute blanket norms, they do not allow for the examining of the interests of each child on a case-by-case basis, or for the taking into account of individual ability and maturity. They are based on a generalized age limit that is used as a proxy for maturity and judgement, and thus may easily exclude children capable of maturely engaging in certain activities. Therefore, it is questionable if a bright-line rule can be justified where it is important to examine the best interests of each child on an individual basis.

3. European effort to adapt children's right to privacy to a 'digital age': two dilemmas

The Regulation attempts to introduce measures to achieve far-reaching changes in relation to the processing of a child's personal data online. The question is, however, whether the Regulation will succeed in guaranteeing the universal child's right to privacy in the online environment while adequately balancing the concerns of online risks and opportunities and accounting for the growing maturity of children.

3.1. Empowerment versus protection in EU data protection law

Since the early days of the Internet, the empowerment versus protection dilemma has been present in child safety policy. Policy makers have been faced with a need to maximize accessibility and opportunities presented by digital spaces while seeking to protect vulnerable Internet users from the potential risks and harm associated with their online activities. Dominant concerns related to child sexual abuse have led to a very protectionist stance in relation to children as Internet users. However, highly paternalistic views have problematic consequences for children as rights holders, 'neglecting their agency and rights to access, information, privacy and participation' (Livingstone et al., 2015: 5).

Despite strong agreement on the need to create policies that balance children's opportunities to access information online with the need to minimize their exposure to safety and privacy risks (Livingstone et al., 2011), achieving this remains a complicated task that requires a careful balancing act. Empirical research demonstrates that opportunities and risks online go together. More Internet usage allows children to gain more digital skills, and to climb the 'ladder of opportunities' (Livingstone and Helsper, 2007). However, children who take up more online activities encounter more risks. These risks may not necessarily result in harm, and may be seen as risky opportunities that 'allow children to experiment online with relationships, intimacy and identity' (Livingstone et al., 2011: 2). On the one hand, these risky opportunities are vital for children in order for them to learn coping behaviour and to build resilience. On the other hand, risky opportunities may lead to vulnerability, depending on the specific

circumstances of the child (socioeconomic and psychological factors) and on the design of the online environment (Livingstone et al., 2011).

Ideally, data protection law should protect children from privacy risks, such as commercial data exploitation and misuse, reputational damage, or harm to one's identity, dignity and personal integrity, while also enhancing online opportunities. This requires a policy framework that not only imposes legal compliance requirements on data controllers, but that also aims to empower children while addressing the needs of those who require greater protection. The Regulation tries to do so with its new empowering and protective provisions. What remains questionable, however, is how successfully it has addressed the empowerment versus protection dilemma, that is, how well does the Regulation strike an adequate balance between the two poles?

3.1.1. Empowering children as Internet users

User empowerment relates to 'the necessary capabilities for interpreting and acting upon a social world that is intensively mediated by the new media' (Mansell, 2002: 409). Pierson (2012: 103) underlines the importance of inclusion, digital literacy and privacy as the main issues that need to be addressed before individuals can become empowered online. Following this understanding of user empowerment, several provisions in the Regulation may be seen as aiming to empower children in the digital environment. These empowering provisions are age generic, that is, they apply equally to both adults and children, but can be framed as specifically relevant to children and their online activities.

3.1.1.1. The right to be forgotten

The most prominent empowering right in the Regulation is the right to be forgotten, a facet of the right to erasure, and an updated and clarified version of the right of access, both already present in the Data Protection Directive (95/46/EC). It is an effort to address the fact that personal information on the Internet can be universally accessed and searched, but not easily removed.

Particularly aimed at children in online environments, when their data is collected based on consent, the right to be forgotten allows children to remove personal information that may be damaging to their reputation and personality. It can be exercised even if an individual is no longer a child. This right is not absolute and does not apply when the data is necessary for the exercise of the right of freedoms of expression and information, archiving purposes or scientific and historical research.

In the ruling of *Google vs Spain* (C-131/12) the EU Court of Justice had already decided that individuals have the right – under certain conditions – to ask search engines to remove links with their personal information that is inaccurate, inadequate, irrelevant or excessive for the original collection purposes. The ruling sparked a wide debate on both sides of the Atlantic due to a possible chilling effect on access to information and free expression.

The application of this right to children may be more problematic than to adults, demanding a dynamic perspective: with time, an unknown child may become a public figure, and his or her data may therefore change status from private (worth deleting) to something worth public interest (worth preserving) (Blume, 2015).

3.1.1.2. The right to data portability

This new right should allow Internet users to shift from one service provider to another by moving their personal data. This, according to the European Commission (EC, 2015), should benefit both individuals and companies, as 'start-ups and smaller companies will be able to access data markets dominated by digital giants and attract more consumers with privacy-friendly solutions'. In fact, an easier exit from 'walled gardens', such as Facebook (Barnett, 2010), can reinforce the ongoing trend of social media platform diversification (Cortesi, 2013) among children, and consequently empower children to choose more privacy-friendly online services.

3.1.1.3. 'Data protection by design' and 'data protection by default'

The 'data protection by design' and 'data protection by default' principles require data protection requirements and safeguards to be built into products and services from the initial stage of their design. Privacy-friendly default settings are expected to be the norm on social networks or mobile apps (EC, 2015), vital for children, as empirical research indicates that on social networking sites (SNSs) 'not everyone has the digital skills to manage privacy and personal disclosure and many 9- to 12-year-olds use SNSs underage, including 20 percent on Facebook and 38 percent using SNSs overall' (Livingstone et al., 2011: 2).

3.1.1.4. Transparent information and awareness

As highlighted by Van Dijk (2013), 'user empowerment is dependent on knowledge of how mechanisms operate and from what premise, as well as on the skills to change them' (p. 171). The Regulation obliges data controllers to give information to all data subjects in a clear, audience-appropriate language, for example, by using standardized icons, and the time that their personal data is collected. Recital 58 frames this requirement in relation to children as giving information 'in such a clear and plain language that the child can easily understand'. The challenge that will be faced by data controllers in practice, however, is how to implement the transparency requirement in a meaningful way in the case of children (Savirimuthu, 2016).

3.1.2. Protecting children as data subjects

Along with a number of empowering provisions, the Regulation introduces two protective provisions, specifically for children as data subjects, that is, subjects whose personal data is collected, held or processed. Protective provisions impose obligations on external parties: negative obligations on data controllers to abstain from certain data collection practices, and positive obligations on parents to engage in activities to secure the effective enjoyment of their child's fundamental rights.

3.1.2.1. Prohibition of profiling

The Regulation prohibits certain potentially harmful data collection and usage practices through restrictions on the activities of data controllers. Recital 38 generally emphasizes that specific protection should be afforded to children against marketing or profiling. Under Article 4(4), 'profiling' means any automated data processing activity that involves (a) automated processing of personal data and (b) using that personal data to evaluate certain personal aspects relating to a natural person, such as personal preferences, interests, behaviour and location. Recital 71 acknowledges that automated decision making based on profiling should not concern children. This leads to the conclusion that the profiling of children is prohibited, even

if the articles of the Regulation do not specifically state so. Given the overarching objective of the GDPR to provide children enhanced protection, it would have been desirable to explicitly exclude children from profiling. The current wording of the GDPR may lead to the interpretation that only automated decisions that produce legal effects or similarly significantly affect the child are absolutely prohibited. The prohibition against creating personality or user profiles of children follows the position of the Article 29 Working Party (A29WP, 2013), which stated that behavioural advertising 'will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing'.

The prohibition of profiling has the potential to diminish the commercial exploitation of children's data that is now happening through complex marketing, tracking and targeting systems used by many online service providers that monitor and monetize children's online behaviour and interactions (Montgomery and Chester, 2015). It may also foster the use of contextual, instead of behavioural, advertising by children's websites and services. Nonetheless, it remains to be seen how effectively such a prohibition can be enforced in practice. For example, Savirimuthu (2016) claims that children might feel only marginal benefits, as profiling is not entirely forbidden in the Regulation and can be carried out in the legitimate interests of the data controller, subject to 'suitable' instead of 'effective' safeguards (p. 244). Also, even though it might be possible to infer that a user is a child using modern profiling and data mining techniques (European NGO Alliance for Child Safety Online [eNACSO], 2016), it is still difficult to reliably distinguish between adults and children online (Van Der Hof, 2014). An obligation to identify children in order to completely remove them from all targeting may lead to excessive data collection of a large number of adults, and instead of protecting one's privacy and anonymity online, it could diminish and erode both.

3.1.2.2 Parental consent

The requirement of prior parental consent or authorization before the processing of the personal data of children when they are directly offered 'Information Society services' (Article 8) is probably the most controversial and important protective provision. As the EC explains, this provision 'aims at protecting children from being pressured to share personal data without fully realising the consequences' (EC, 2015). As a general rule, protection through the parental consent mechanism is applicable to children under the age of 16. However, 16 years is not an absolute threshold, as member states are allowed to apply a lower age limit, which nevertheless cannot be lower than 13 years.[2] The parental consent requirement is applicable online, excluding offline data processing practices, such as those in the context of school or leisure activities. However, virtual and physical realities are frequently entirely intertwined and mixed for children, creating one total 'inter-reality' (Van Kokswijk, 2007: 40), and thus the consent requirement will significantly affect the daily lives of many children.

The default age of 16 is the most debatable legislative choice, raising concerns of being too inclusive and over-protective for several reasons. First, the consent requirement in the Regulation is fully applicable. Instead of protecting the most vulnerable Internet users from harm, it risks limiting all children in their online activities and restricting their opportunities. Except for the preventive or counselling services offered directly to a child, an area where children and parents may often have conflicting interests, or where the parental consent requirement could cause a delay in an emergency situation, the Regulation does not foresee consent exceptions for less risky data collection practices. Rather than being subject to one

single rule, the consent requirement could foresee several different scenarios. For example, nuanced risk-based requirements for parental consent exists in the US Children's Online Privacy Protection Act (COPPA) and could have been considered by the EU legislator. Under COPPA, commercial services that are not interactive or do not share children's personal data need not obtain parental consent. Where a service uses children's data for internal purposes, it has to employ a lighter consent mechanism, such as the sending of an email to the parent and taking an additional confirming step after receiving the parent's response ('email plus' method). The highest risk services are those that disclose personal data to third parties, use behavioural advertising and enable children to publicly post information. These services must comply with the most rigid consent mechanisms, such as parents filling in and returning consent forms by mail, fax or scan, the provision of a credit card number, contacting the service provider via a toll-free number or video conference, and the verification of an official identification document.

Second, the consent rule is very broad in scope. An Information Society service is 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services'.[3] As a result, consent will be sought from parents for all types of services in different sectors, that not only include social media, but also online gaming, entertainment sites, instant messaging and email services (Jasmontaite and De Hert, 2014). Some of these services have nothing to do with disclosing personal data online or behavioural tracking, the main worries that seem to be driving the establishment of a specific child data protection regime. An overload of consent requests may result in 'consent fatigue' among parents, when a constant consenting process becomes a disturbing irritation rather than a serious choice. This can make the entire parental consent provision illusionary.

Third, the UN CRC obliges state parties to encourage, through legislation and policy, parents 'to listen to children and give due weight to their views in matters that concern them' (CRC, 2009). However, the consent requirement in the Regulation positions parents as arbiters in deciding what is both allowed and beneficial for their children, without formally allowing children to influence their decisions. Such a concentration of decisional power placed in the hands of parents raises several issues. Parents may not always be in a position to fully grasp the best interests of the child. There could be cases of disagreement between parents and children over the usefulness and risks in relation to social media, and emotional, moral panic-driven or simply unjustified consent request rejections from parents. According to boyd (2014), adults are not always able to understand the positive and complex interactions between technology and young people. Empirical evidence shows that 'one in three parents (51 percent of parents of 9- to 12-year-olds, 15 percent of parents of 13- to 16-year-olds) do not want their child to use SNSs' (Livingstone et al., 2011: 19), even if social media has become a space for the exercise of the freedom of expression, access to information, civic engagement and public participation for children and young people (boyd, 2014). Even worse, parents may become potential invaders of their children's privacy. For example, by using the right of access to personal data on behalf of their children, parents could get to know about their children's online activities (Hoofnagle, 2016). Also, parental consent mechanisms may become parental control systems restricting the online freedoms of children (Van Der Hof, 2014). These concerns are not reflected in the logic of the Regulation, even if the right to privacy of children against their parents and the complexity of privacy boundaries within the family have been evidenced by academics (Newell et al., 2015; Shmueli and Blecher-Prigat, 2011).

Fourth, the Regulation fails to respect the evolving capacities of children, especially older children, and to formally involve them in decisions related to the use of their personal data. It makes no effort to adopt a sliding scale approach, and therefore to increasingly recognize the agency of children, foster the participation of children in their own protection and support coping and resilience through learning by doing. Freeman (1983) wisely states that special treatment can be justified due to a child's incapacity and immaturity, but at the same time, children should be brought to 'a capacity where they are able to take full responsibility as free, rational agents for their own system of ends' (p. 57). The Regulation contradicts the right of children to be heard and taken seriously, enshrined in the UN CRC and EU Charter of Fundamental Rights. The Committee on the Rights of the Child (2009) has defined Article 12 of the UN CRC (the right to be heard) not only as a right but also as a general principle – that is, this article should be considered in the interpretation of all other child rights. It requires recognizing that children are gradually capable of contributing to decisions about them, such as the use of their images or the monitoring of their activities, and should be consulted accordingly (A29WP, 2009). In the Regulation, solutions for consent could have varied from mere consultation of the child, to the parallel or joint consent of the child and a parent, and even to the autonomous consent of a mature child (A29WP, 2009).

3.2. Individualized versus average child dilemma

Determining a precise age limit after which the processing of personal data becomes subject to fewer legal constraints is not a challenge faced solely by data protection law. Other areas such as family, civil, criminal and administrative law have also faced the question of whether a line indicating a particular age as the starting point of adulthood had to be drawn. Sometimes the law looks at the issue on a case-by-case basis, examining factors particular to the individual child, and in other situations the law adopts a bright-line (i.e. age of 14, 16, 18 years) rule. This is essentially a choice to be made in the 'individualized vs average child' dilemma.

The Regulation chooses to set a single age when all children can be deemed competent to consent to the processing of their personal data, relying on an 'average child' criteria. Such a legislative choice of determining a prescribed age limit can be criticized for several reasons.

First, the capacities of a child are personal, context-dependent and constantly evolving. An assessment in each individual case would show widely differing capacities among children of the same age and could, thereby, reflect the best interests of the child.

In fact, presently, only three member states (Spain, Hungary and the Netherlands) have chosen to explicitly state in their national data protection law the exact age threshold for consent.[4] Many remaining member states rely on the individualized child criteria and advise data controllers to perform a subjective and context-specific rather than universally applicable capacity test. In order to decide whether a child is able to consent, the data controllers should assess the concrete situation on a case-by-case basis, applying general criteria of the best interests of the child, level of moral and psychological development, the capacity to understand the consequences of giving consent and evaluating specific circumstances (age of the child, purpose of data processing, type of personal data involved, etc.). Only exemplar assumption-based age thresholds are sometimes set in case law, legal doctrine or guidelines from the data protection authorities. On the European level, national data protection authorities took a

similarly flexible approach and did not set precise age limits at which parental consent is required. Instead, they underlined the importance of the maturity of a child and complexity of the data processing at hand (A29WP, 2009).

Second, the same child may need protection for one data processing purpose, and autonomy or self-determination for another, depending on the potential privacy risks and harm that are at stake. For instance, data collection for the purpose of sending a newsletter might not require parental consent, while such consent would be necessary to create a social media account in relation to the same child (UK Information Commissioner's Office [ICO], 2010). The imposition of legal age limits may disproportionally restrict the rights of other children and data subjects, irrespective of a child's own levels of competence.

3.3. More protection or empowerment?

At first glance, the Regulation seems to provide many innovative empowerment rights, while failing on protective rights for children. A closer look, however, reveals that paternalistic protection is a favoured approach in the Regulation over the empowerment of children. The Regulation justifies protective measures exclusively in light of children's inadequacies by stating that children merit specific protection due to their potentially lower awareness of risks, consequences, safeguards and rights relating to the processing of their personal data (Recital 38).

More importantly, although particularly relevant to children, all the empowering provisions in the Regulation are addressed to individuals of all ages, while only the protective provisions apply exclusively to children. In what Stalford (2012) calls the 'hegemony of child protection', the strict consent requirement formulated in Article 8 of the Regulation seems to place children under the strict over-protection of their parents (p. 224). As a consequence, Article 8 does not address the weight to be assigned to the child's opinion, nor does it acknowledge the interrelation between a child's opinion and his or her best interests. The adoption of broad parental oversight through the consent mechanism also raises questions as to whether and to what extent children will be able to enjoy the empowering rights, such as the right to be forgotten and data portability, without parental involvement. In sum, the highly protective consent provision seems to distort the balance between empowerment and protection towards the latter, especially for teens.

4. A look to the future – beyond the letter of the law

Despite the promising rights and obligations related to children in the Regulation, in reality, only their proper and effective implementation will demonstrate any credible attempt from the EU to empower and protect children. In order to reach such implementation, a number of complex, practical, structural and intellectual challenges are to be addressed by EU policy makers, national data protection authorities and Information Society service providers.

The biggest practical challenge for the EU will be to ensure that online a child's age and parental consent are verifiable, or the main protective provision in the Regulation will lose its effectiveness. As a side effect, an unenforced legal requirement on parental consent might lead to the loss of respect for the mere idea of rule-making (eNACSO, 2016). Up until now, there

have been no foolproof, adequate mechanisms to universally verify a child's age online. Determined children are able circumvent the majority of age verification mechanisms by simply lying about their age or pretending to be their parents without penalty. Ideally, to avoid overburdening, age verification would be based on a sliding scale approach and depend on the circumstances, such as data processing purpose and use and type of data (A29WP, 2011). Although consent verification techniques exist, they have to be both effective and easy to use, as well as having to comply with the main data protection principles, such as data minimization, purpose limitation, data adequacy and relevance (Jasmontaite and De Hert, 2014).

The Regulation encourages data controllers to determine techniques for verifiable parental consent in the codes of conduct of industry associations. Until now, the success of such voluntary codes in practice has been very limited. The number of codes approved by the national data protection authorities varies from one member state to another. On the European level, very few organizations representing specific sectors have tried, and only one of them has managed to draw up a code that was fully endorsed by the European data protection authorities.[5] Self-regulatory codes are often limited in their ability to protect children, because of vague language, inadequate enforcement and monitoring mechanisms (Macenaite, 2016). Alternative approaches, such as explicitly integrating the UN CRC principles into self-regulatory codes, instead of leaving the industry to determine their standards for respecting children's needs and interests, could provide valuable solutions (Savirimuthu, 2016). Stronger participation of the EU public authorities in the self-regulatory process, in particular, rule formulation and enforcement, could help to achieve a better balance between the interests of children to exercise control over their personal data and the desire of businesses to valorize and profit from users' personal data.

More fundamentally, it should be acknowledged that, on a structural level, informed consent to personal data processing is not a panacea tantamount to giving complete control to individuals over their personal data in complex networked environments. A rich body of literature points to the characteristics of the networked environments that restrain an individual's control over their personal data (Cohen, 2012; Hildebrandt, 2008). Various scholars have emphasized the weaknesses of consent as a protection mechanism online (Mantelero, 2014; Schermer et al., 2014). Neither parents nor children can take full responsibility and control of their personal data online, as their choices and data control possibilities are shaped by the design and functionalities of communication spaces (Marwick and boyd, 2014). Although there is no easy answer to the structural power imbalances online, privacy enhancing engineering and design solutions, if enforced under the data protection by design obligations of the Regulation, could provide some realistic possibilities to affect networked environments and respond to children's needs and expectations.

Finally, an intellectual challenge for member states will be to define an average child in different data collection scenarios based on comprehensive research and solid empirical evidence. Social and behavioural sciences should be the first areas from which national legislators should gather the evidence to justify any given age limit. As it seems highly unlikely that fixing a single age limit for consent in all data processing activities online could be the most appropriate solution, different sectors, data collection practices and age spans might require detailed examination and research. In addition, the views of children themselves should be considered in policy making, preparation of national laws related to the processing of children's personal data, as well as their evaluation (CRC, 2009).

Notes

1. The Regulation was adopted on 14 April 2016, after more than 4 years of debate. It will come into force from 25 May 2018.
2. Previous drafts of the Regulation, consistently with Children's Online Privacy Protection Act (COPPA), foresaw 13 as the age of consent. A last minute change during the European Union (EU) trilogue negotiations, which raised the age to 16, generated public outrage. The provision has been interpreted as banning children from social media and even as being an attack on their human rights, such as freedom of expression and right to information.
3. Point (b) of Article 1(1) of the Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241 2015).
4. Parental consent is required for the processing of personal data of children under the age of 14 in Spain (Article 13 of the Spanish Royal Decree 1720/2007 of 21 December) and 16 in the Netherlands (Article 5 of the Dutch Personal Data Protection Act [25 892] of 23 November 1999) and Hungary (Section 6[3] of the Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information).
5. The European codes of practice for the use of personal data in direct marketing by Federation of European Direct and Interactive Marketing (FEDMA), including an annex on online direct marketing (www.fedma.org/index.php?id=56).

References

Article 29 Working Party (A29WP) (2009) Opinion 2/2009 on the protection of children's personal data (general guidelines and the special case of schools). WP 160, 11 February. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf

Article 29 Working Party (A29WP) (2011) Opinion 15/2011 on the definition of consent. WP 187, 13 July. Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Article 29 Working Party (A29WP) (2013) Opinion 02/2013 on apps on smart devices. WP 202, 27 February. Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf

Barnett E (2010) Tim Berners-Lee criticises Facebook's 'walled garden'. *The Telegraph*, 22 November. Available at: www.telegraph.co.uk/technology/facebook/8151101/tTim-Berners-Lee-criticises-Facebooks-walled-garden.html

Blume P (2015) The data subject. *European Data Protection Law Review* 1(4): 258–264.

boyd d (2014) *It's Complicated: The Social Lives of Networked Teens*. New Haven, CT: Yale University Press.

Boyden J and Levison D (2000) Children as economic and social actors in the development process. EGDI working paper. Stockholm: Expert Group on Development Issues. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.120.1198&rep=rep1&type=pdf

Cohen JE (2012) *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven, CT: Yale University Press.

Committee on the Rights of the Child (CRC) (2009) The right of the child to be heard. CRC/C/GC/12. Available at: http://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/CRC-C-GC-12.pdf

Cortesi S (2013) Youth online: diversifying social media platforms and practices. In: Gasser U, Faris R and Heacock R (eds) *Internet Monitor 2013: Reflections on the Digital World*. Berkman Center Research Publication 27. Cambridge: the Berkman Center for Internet & Society at Harvard University, pp. 16–17.

Douglas M (2013) *Rules and Meanings*. London: Routledge.

Eekelaar J (1986) The emergence of children's rights. *Oxford Journal of Legal Studies* 6(2): 161–182.

European Commission (EC) (2015) Stronger data protection rules for Europe. Fact sheet. Available at: http://europa.eu/rapid/press-release_MEMO-15-5170_en.htm

European Court of Human Rights (ECHR) (2006) *Evans v United Kingdom*. Application number 6339/05. Strasbourg: ECHR.

European NGO Alliance for Child Safety Online (eNACSO) (2016) *When Free Isn't: Business, Children and the Internet*. Rome: eNACSO. Available at: www.enacso.eu/wp-content/uploads/2015/12/free-isnt.pdf

Federle KH (2013) *Children and the Law: An Interdisciplinary Approach with Cases, Materials and Comments*. New York: Oxford University Press.

Fortin J (2009) *Children's Rights and the Developing Law*. Cambridge: Cambridge University Press.

Freeman MDA (1983) *The Rights and Wrongs of Children*. London: Dover.

Freeman MDA (1993) Laws, conventions and rights. *Children & Society* 7(1): 37–48.

Gilmore S and Glennon L (2014) *Hayes and Williams' Family Law*. Oxford: Oxford University Press.

Hildebrandt M (2008) Profiling and the rule of law. *Identity in the Information Society* 1(1): 55–70.

Hoofnagle C (2016) *Federal Trade Commission Privacy Law and Policy*. New York: Cambridge University Press.

Jasmontaite L and De Hert P (2014) The EU, children under 13 years and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet. *International Data Privacy Law* 5(1): 20–33.

Lansdown G (2005) *The Evolving Capacities of the Child*. Florence: UNICEF Innocenti Research Centre.

Livingstone S and Helsper E (2007) Gradations in digital inclusion: children, young people and the digital divide. *New Media & Society* 9(4): 671–696.

Livingstone S, Carr J and Byrne J (2015) *One in three: Internet governance and children's rights*. Global commission on Internet governance paper series no. 22. London: Centre for International Governance Innovation.

Livingstone S, Haddon L, Görzig A, et al. (2011) *Risks and safety on the Internet: the perspective of European children*. Full findings. London: EU Kids Online, LSE.

McGlynn C (2002) Rights for children: the potential impact of the European Union charter of fundamental rights. *European Public Law* 8(3): 387–400.

Macenaite M (2016) Protecting children's privacy online: a critical look to four European self-regulatory initiatives. European Journal of Law and Technology 7(2): 1-26.

Mansell R (2002) From digital divides to digital entitlements in knowledge societies. *Current Sociology* 50(3): 407–426.

Mantelero A (2014) The future of consumer data protection in the EU: rethinking the 'notice and consent' paradigm in the new era of predictive analytics. *Computer Law & Security Report* 30: 643–666.

Mantelero A (2016) Children online and the future EU data protection framework: empirical evidences and legal analysis. *International Journal of Technology Policy and Law* 2(2–4): 169–181.

Marwick AE and boyd d (2014) Networked privacy: how teenagers negotiate context in social media. *New Media & Society* 16: 1051–1067.

Montgomery K and Chester J (2015) Data protection for youth in the digital age: developing a rights-based global framework. *European Data Protection Law Review* 1(4): 277–291.

Newell BC, Metoyer C and Moore AD (2015) Privacy in the family. In: Roessler B and Mokrosinska D (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge: Cambridge University Press, pp. 104–121.

Pierson J (2012) Online privacy in social media: a conceptual exploration of empowerment and vulnerability. *Communications and Strategies* 4(88): 99–120.

Savirimuthu J (2016) Networked children, commercial profiling and the EU data protection reform agenda: in the child's best interests? In: Iusmen I and Stalford H (eds) *The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions*. Opladen: Barbara Budrich Publishers, pp. 221–257.

Scarre G (1980) Children and paternalism. *Philosophy* 55(211): 117–124.

Schermer BW, Custers BHM and Van Der Hof S (2014) The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology* 16(2): 171–182.

Shmueli B and Blecher-Prigat A (2011) Privacy for children. *Columbia Human Rights Law Review* 42: 759–795.

Stalford H (2012) *Children and the European Union: Rights, Welfare and Accountability*. Oxford: Hart Publishing.

UK Information Commissioner's Office (ICO) (2010) Personal information online code of practice. Available at: https://ico.org.uk/media/for-organisations/documents/1591/personal_information_online_cop.pdf

United Nations (UN) (1989) *Convention on the Rights of the Child*. Geneva: Office of the United Nations High Commissioner for Human Rights. Available at: www.ohchr.org/en/professionalinterest/pages/crc.aspx

Van Der Hof S (2014) No child's play – online data protection for children. In: Van Der Hof S, Van Den Berg B and Schermer B (eds) *Minding Minors Wandering the Web: Regulating Online Child Safety. Information Technology & Law Series No. 24*. The Hague: Springer Press/TMC Asser Press, pp. 127–141.

Van Dijk J (2013) *Culture of Connectivity: A Critical History of Social Media*. Oxford: Oxford University Press.

Van Kokswijk J (2007) *Digital Ego: Social and Legal Aspects of Virtual Identity*. Delft: Eburon Uitgeverij.

Chapter 3

Consent for processing children's personal data in the EU: following in US footsteps?

Published in a peer-reviewed journal as:

Macenaite M., Kosta E., Consent for processing children's personal data in the EU: following in US footsteps?, 26(2) Information & Communications Technology Law, 2017, 146-197.

Abstract

With the recent adoption of the General Data Protection Regulation (GDPR), the European Union assigned a prominent role to parental consent in order to protect the personal data of minors online. For the first time, the GDPR requires parental consent before information society service providers can process the personal data of children under 16 years of age. This provision is new for Europe and faces many interpretation and implementation challenges, but not for the US, which adopted detailed rules for the operators that collect personal information from children under the Children's Online Privacy Protection Act (COPPA) almost two decades ago. The article critically assesses the provisions of the GDPR related to the consent of minors, and makes a comparative analysis with the requirements stipulated in the COPPA in order to identify pitfalls and lessons to be learnt before the new rules in the EU become applicable.

Keywords: children, consent, data protection, General Data Protection Regulation, COPPA.

1. Introduction

Children are actively present online at an ever-younger age. It is estimated, that globally one in three internet users are under the age of 18.[97] Online, children not only enjoy exciting opportunities of playing, creating, learning, self-expressing, experimenting with relationships and identities, but are also disclosing increasing amounts of their personal data. Ubiquitous computing and the increasing datafication of everything[98] is seen as enhancing online privacy risks, such as commercial exploitation and misuse of personal data, profiling, identity theft, the loss of reputation and discrimination. For example, as the consequence of dataveillance

[97] Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' (2015) Global Commission on Internet Governance Paper Series No. 22.

[98] Viktor Mayer-Schönberger and Kenneth Neil Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013)

practices via wearable and mobile devices, social media platforms, and educational software, "children are configured as algorithmic assemblages (…) with the possibility that their complexities, potentialities and opportunities may be circumscribed".[99] In addition, due to their particular behavioural characteristics, emotional volatility and impulsiveness, children (especially teenagers) are seen as being more vulnerable in comparison to adults online.[100] Developmental psychology provides evidence that adolescents can be more active and risk-prone online.[101] They may be less capable of evaluating perilous situations and can be more easily misled, given their lack of awareness vis-à-vis the long-term consequences of their virtual actions.[102] These specific developmental features of children might be easily exploited by online marketers who collect personal data and employ special techniques such as "real-time bidding, location targeting (especially when the user is near a point of purchase), and "dynamic creative" ads tailored to their individual profile and behavioral patterns"[103].
Empirical studies show that privacy risks are common on the internet[104] and privacy concerns constitute one of the main worries among children in Europe.[105] In the same vein, adults widely support the introduction of the special data protection measures for children. According to an Eurobarometer survey, 95% of Europeans believed that "under-age children should be specially protected from the collection and disclosure of personal data" and 96% thought that "minors should be warned of the consequences of collecting and disclosing personal data".[106]

Given these online risks and public concerns, there have been increasing calls from policy-makers and academics to transform children's rights, in particular the rights guaranteed by the UN Convention on the Rights of the Child (UN CRC), to cater for the 'digital age'.[107] Among

---

[99] Deborah Lupton and Ben Williamson, 'The datafied child: The dataveillance of children and implications for their rights' (2017) New Media & Society (forthcoming) <http://journals.sagepub.com/doi/abs/10.1177/1461444816686328 > accessed 1 April 2017.

[100] Judith Bessant, 'Hard wired for risk: neurological science, 'the adolescent brain' and developmental theory', (2008) 11(3) Journal of Youth Studies 347, 358 (criticises research on adolescent brain as "it begins with a prejudice ('they' are 'different' 'irrational' and 'deficient') and then threatens to expand the civil and social disadvantages that already severely affect too many of our young people". Bessant claims that "some young people are sometimes at risk not because their brains are different, but because they have not had the experience or opportunity to develop the skills and judgment that engagement in those activities and experiences supply".)

[101] Andrew Hope, 'Risk-taking, boundary-performance and intentional school internet 'misuse'', (2007) 28(1) Discourse: studies in the cultural politics of education 87.

[102] Jay N Giedd, 'The Teen Brain: Insights from neuroimaging', (2008) 42(4) Journal of Adolescent Health 335; Elizabeth R McAnarney, 'Adolescent Brain Development: Forging New Links?' (2008) 42(4) Journal of Adolescent Health 321; Tim McCreanor et al. 'Consuming identities: Alcohol marketing and the commodification of youth experience', (2009) 13 (6) Addiction Research & Theory 579; Laurence Steinberg, 'Risk taking in adolescence: New perspectives from brain and behavioral science', (2007) 16 (2) Current Directions in Psychological Science 55; Laurence Steinberg, 'Social neuroscience perspective on adolescent risk-taking' (2008) 28(1) Developmental Review 78.

[103] Kathryn C. Montgomery, 'Youth and surveillance in the Facebook era', (2015) 39(9) Telecommunications Policy 771; Kathryn C Montgomery and Jeff Chester, 'Data protection for youth in the digital age: Developing a rights-based global framework', (2015)1(4) European Data Protection Law Review 291.

[104] For example, according to the empirical data of the EU Kids online, 9% of children aged 11-16 in Europe have experienced personal data misuse online. See Sonia Livingstone et al., 'Risks and safety on the Internet: The perspective of European children' (LSE, EU Kids Online, London 2011).

[105] Giovanna Mascheroni and Kjartan Ólafsson, *Net children go mobile: risks and opportunities* (2nd edn Educatt, Milan 2014)

[106] European Commission, 'Special Eurobarometer 359: Attitudes on Data Protection and Electronic Identity in the European Union' (June 2011) <http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> 196 and 203.

[107] Council of Europe, Strategy for the Rights of the Child (2016-2021) (March 2016); UN Committee on the Rights of the Child, Report of the 2014 Day of General Discussion 'Digital media and children's rights', (May 2015); UNICEF, 'Privacy, protection of personal information and reputation rights' (2017)

the rights to provision and participation, the UN CRC recognises children's rights to protection, including a specific protection against arbitrary or unlawful interference with children's privacy, and unlawful attacks on their honour and reputation (Article 16).[108]

Yet, protection of informational privacy in the EU has been designed for "everyone", conflating adults and children in one single group of data subjects. Since 1995, minors are covered by the age-generic data protection provisions provided by Directive 95/46/EC with no special focus on the processing of children's data. The newly adopted EU General Data Protection Regulation (2016/679)[109] (hereinafter - 'GDPR' or 'Regulation') has significantly changed the *status quo* and rejected the "age-blind" approach to data subjects. The GDPR, which has faced long debates during its adoption process[110], explicitly recognizes that children need more protection than adults. As explained by Recital 38 of the GDPR, children merit special protection as they "may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data", especially online. To provide such special protection, the GDPR has introduced far-reaching changes in relation to the processing of minor's personal data online, such as child-appropriate information, a stricter right to erasure, and stronger protection against marketing and profiling.[111] Most importantly and controversially, in cases when the processing of personal data of children takes place on the basis of consent (in accordance with Article 6(1)(a) GDPR), Article 8 of the GDPR has established a parental consent requirement before the offering of 'information society services'

Discussion paper <https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf> accessed 5 April 2017; UK Children's Commissioner, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (January 2017) <http://www.childrenscommissioner.gov.uk/sites/default/files/publications/Growing%20Up%20Digital%20Taskforce%20Report%20January%202017_0.pdf> accessed 9 April 2017; UK House of Lords Committee on Communications, 'Growing up with the internet' (2nd Report of Session 2016–17) (March 2017), <https://www.publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/130.pdf> accessed 9 April 2017; Sonia Livingstone and Amanda Third, 'Children and young people's rights in the digital age: an emerging agenda' (2017) New Media & Society (forthcoming); Sonia Livingstone and Brian O'Neill, 'Children's rights online: challenges, dilemmas and emerging directions' in Simone van der Hof, Bibi van den Berg and Bart Schermer, (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Information technology and law series (24) (Springer with T. M. C. Asser Press, The Hague, 2014) 19.

[108] United Nations Convention on the Rights of the Child (20 November 1989, 1577 UNTS 3 (UN CRC).

[109] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[110] Data Protection revision process has started on 25 January, 2012, when the European Commission, amongst others, published a Proposal for a General Data Protection Regulation (GDPR). On 21 October, 2013 the LIBE Committee of the European Parliament voted on the Draft Report prepared by the rapporteur Jan Philipp Albrecht. On 12 March, 2014 LIBE Report has been adopted by the European Parliament. On 15 June, 2015 the Council agreed on General Approach and on 9 November 9, 2015 on its negotiating position. On 15 December, 2015 the Parliament and the Council reached political agreement in trilogue. On 17 December 17, 2015 LIBE Committee voted on texts agreed during interinstitutional negotiations. On 8 April, 2016 the Council adopted its Position and Statement of the Council's reasons. On 12 April, 2016 LIBE Committee voted on Recommendation for 2nd reading and on 14 April, 2016 the Parliament adopted the GDPR in 2nd reading. On 27 April, 2016 GDPR was signed and on 4 May, 2016 published in the Official Journal of the European Union.

[111] For a more detailed description of the child specific protection regime in the GDPR see Milda Macenaite, 'From universal towards child-specific protection of the right to privacy online: dilemmas in the EU General Data Protection Regulation' (2017) New Media and Society (forthcoming) <https://doi.org/10.1177/1461444816686327> accessed 1 April 2017.

directly to children under the age of 16 (unless a lower national age threshold between 13 and 16 applies).

Being new, the GDPR's parental consent requirement remains unclear and faces many practical implementation challenges. However, in the US since 1998 the Children's Online Privacy Protection Act (COPPA) has provided detailed rules for the operators of online services directed towards children that collect (or have actual knowledge that they collect) personal information from children. As the GDPR has been partially inspired by COPPA, US experience could inform the debate in the EU over the new data protection challenges related to children's consent in relation to online services. Thus, the aim of this article is to critically assess the provisions of the GDPR related to the consent of minors, and make a comparative analysis with the requirements stipulated in the US COPPA in order to identify pitfalls and lessons to be learnt before the new rules on the consent of minors in the EU become applicable.

This article is divided in five parts. The first part provides an overview of the context relating to the processing of children's personal data, especially in the online world. The second part explores the general notion of consent in the EU data protection law, including the conditions for a valid consent. In the third part, the legislative development of Article 8 of the GDPR dealing specifically with children's consent in relation to information society services is examined. The fourth part presents the US relevant legislative framework, i.e. COPPA and its main requirements. In the fifth part, the challenges related to the practical implementation of the provision on the consent of minors in the GDPR will be discussed in light of the US experience. Finally, based on this comparison, we will conclude with some recommendations for the future application of the new rules on the consent of minors.

2. Conception of article 8 – Exploring the context

Since the adoption of Directive 95/46/EC in the pre-internet era which remained silent in relation to children, the regulatory context for the GDPR has drastically changed. In particular, there have been several driving factors (contextual and legal) behind the vast increase in attention for children's privacy protection on the Internet, that played a role in acknowledging children as special data subjects in the GDPR .

2.1. Contextual developments

Several developments can be seen as preparing the ground for the adoption of specific provisions in the GDPR relating to the protection of minors with regard to the processing of their personal data.

First, in recent years increased attention has been paid to children and their rights in EU policy making. The importance of promoting children rights has become a clear objective of the EU as stated in Article 3(3) of the TEU. In Article 24 of the European Charter of Fundamental Rights, the EU committed to safeguarding children's rights to protection and care. Moreover, the effective protection of children in all EU policies having an impact on their rights are

identified among the main priorities in EU strategic documents.[112] These documents transform the EU policy objectives into actions. The need to ensure that children's rights are enhanced and respected in all the EU legislative proposals and decisions has been continuously acknowledged among the EU institutions. In fact, the EU Agenda for the Rights of the Child recognises as one of its objectives the achievement of "a high level of protection of children in the digital space, including of their personal data, while fully upholding their right to access internet for the benefit of their social and cultural development".[113] In 2015, the European Parliament and the Council called on the European Commission to present a new and comprehensive strategy and action plan on the rights of the child.[114] The commitment of the EU institutions to promoting, protecting and fulfilling children's rights in all relevant policy areas and actions means that the principles of the UN CRC should guide the EU policies directly or indirectly affecting children. In other words, children's rights considerations, such as the best interest of the child, should be taken into account in the drafting of legislative proposals.

Second, a significant increase in empirical data about children's internet use and related online risks has been gathered across Europe by the EU funded EU Kids Online project and became available for policy makers, academics and other stakeholders. In 2011, research indicated that 9% of children aged 11-16 experienced personal data misuse online and significant amount of children faced difficulties when finding and using reporting tools and privacy settings to protect themselves online.[115] In 2014, research reaffirmed that some of the most important concerns among children still remain related to personal data misuse and reputational damage, such as hacking of social media accounts, creation of fake profiles, and impersonation.[116]

Third, several inspections on the ground raised the concerns around a growing number of websites and mobile apps targeted at, or frequently used by, ever younger children and the lack of specific data protection rules that would take into account the unique needs of children as data subjects. In 2012, the FTC in the US reviewed information provided to users by 400 kids' apps and revealed that many of them lacked transparency and clear disclosure about the

[112] Commission (EC), 'European Strategy for a Better Internet for Children' (Communication) COM/2012/0196 final, 2 May 2012; Commission (EC), 'An EU Agenda for the Rights of the Child' (Communication) COM/2011/0060 final, 15 February 2011 (establishes the strong commitment of all EU institutions and of all EU Member States to promoting, protecting and fulfilling the rights of the child in all relevant EU policies, states that the standards and principles of the United Nations Convention on the rights of the child must continue to guide EU policies and actions that have an impact on the rights of the child, urges to take the "child rights perspective" into account in all EU measures affecting children).

[113] Commission (EC), 'An EU Agenda for the Rights of the Child', COM/2011/0060 final, 15 February 2011, 10.

[114] European Parliament (EP), Resolution on the 25th anniversary of the UN Convention on the Rights of the Child, 2014/2919(RSP), 27 November 2014 (called on the Commission to present 'an ambitious and comprehensive child rights strategy and action plan for the next five years'); Council of the European Union, Conclusions on the promotion and protection of the rights of the child, 15559/14, 4-5 December 2014 (called on the Commission to develop a renewed EU Agenda for the Rights of the Child in line with Better Regulation principles). Anna Maria Corazza Bildt et al., Question for written answer to the Commission on Child Rights Strategy (2015-2020), E-005691-15, 9 April 2015, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2015-005691+0+DOC+XML+V0//EN> accessed 9 April 2017.

[115] Sonia Livingstone et al., 'Risks and safety on the Internet: The perspective of European children' (LSE, EU Kids Online, London 2011); Sonia Livingstone et al., 'Towards a better internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition' (LSE, EU Kids Online, London 2012).

[116] Giovanna Mascheroni, Kjartan Ólafsson, *Net children go mobile: risks and opportunities* (2 ed Educatt, 2014).

children's data collection practices.[117] In 2015 during the time the GDPR was under debate in the Council, 29 data protection authorities from around the world carried out a Global Privacy Sweep (i.e. a joint review of 1494 websites and apps directed towards children).[118] The results revealed many problems, such as inadequate, non-child-tailored privacy policies, excessive collection of personal data from children, and the frequent disclosure of children's data to third parties. In relation to age verification and parental consent in services, the Sweep report stated that "although many sites and apps claimed in their privacy policies to preclude access to children under a specified age, only 15% of websites and apps swept had age verification or gating to bar younger children from accessing the site or app. Sweepers also found that some of those controls did not function (e.g., a child indicating she was 10 years old could still access the site) and others were only passive (e.g., a pop-up indicating that a child below a specified age should not access the site). Noteworthy, only 24% of sites and apps swept encouraged parental involvement."[119] In response to these finding, some data protection authorities, such as the French data protection authority (CNIL), published guidelines[120] thereby sending a reminder to child-directed websites and services regarding their obligations in terms of *inter alia* parental consent for the collection of sensitive data and photographs from children and the transferring of data to third parties for marketing purposes. In the wake of the EU data protection reform, the results of the sweep could have helped to crystalize the final position on the protection of children's personal data online among the policy makers.

2.2. Lack of harmonisation within the EU

The Directive 95/46/EC failed to explicitly address the age limit of consent and as a result there has been lack of clarity on the matter in many EU countries. The question "at what age can children consent to have their personal data processed" even became ironically called "the million euro question" by European data protection experts.[121] Lack of harmonisation across the EU caused legal uncertainty among data controllers who were exposed to diverging legal rules when collecting children's personal data.[122] In the following paragraphs we will

[117] Federal Trade Commission (FTC), 'Mobile Apps for Kids: Current Privacy Disclosures are Disappointing', (Staff report), February 2012, <https://www.ftc.gov/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing > accessed 9 April 2017. FTC, 'Mobile Apps for Kids: Disclosures Still Not Making the Grade', December 2012, <http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf> accessed 9 April 20

[118] GPEN, '2015 GPEN Sweep - Children's Privacy', 2015, <http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf> accessed 9 April 2017.

[119] Ibid.

[120] Commission Nationale de l'Informatique et des Libertés (CNIL), 'Editeurs de sites pour enfants: n'oubliez pas vos obligations!', 2 September 2015, <https://www.cnil.fr/fr/editeurs-de-sites-pour-enfants-noubliez-pas-vos-obligations-0> accessed 9 April 2017.

[121] Giovanni Buttarelli, 'The Children Faced with the Information Society', 1st Euro Ibero American Seminar On Data Protection: ″Children′s Protection″ Cartagena de Indias (2009) <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Speeches/2009/09-05-26_Cartagena_children_protection_EN.pdf> accessed 9 April 2017.

[122] European Data Protection Supervisor (EDPS), Opinion on the Communication 'A comprehensive approach on personal data protection in the European Union', 2011, <https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf> accessed 9 April 2017 (the EDPS claimed that the GDPR should include specific provisions on children to better protect their particular interests and provide legal certainty for data controllers).

explore why setting the age of consent is a difficult issue and how this issue has been approached by national policy makers in the EU.

2.2.1. The concept of child and his legal capacity

Determination of the legal competence of minors to consent to data processing is a complicated task. The complexity of setting an age specific competence threshold stems from conceptions of childhood, including the ideas about children's needs and capacities and how they change with growth,[123] as well as national historical, cultural and social heritage of a particular country and legal system. In addition, as Hodgkin and Nowell have rightly noted "setting an age for the acquisition of certain rights or for the loss of certain protections is a complex matter [which] balances the concept of the child as a subject of rights whose evolving capacities must be respected with the concept of the State's obligation to provide special protection".[124]

Establishing a precise age limit after which the processing of personal data becomes subject to fewer or no additional legal constraints is not a challenge faced solely by data protection law. Other areas such as consumer contract law, family, civil, criminal, and administrative law, have also faced the question of whether, and if so, where a line indicating a particular age as the starting point of adulthood should be drawn. The UN CRC makes use of the term "child", which it defines as "every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier". This position was also followed by the Article 29 Working Party, which considered a child as someone under the age of 18, unless they have acquired legal adulthood before that age. The European Commission's draft GDPR proposal incorporated the definition of the UN CRC, but this did not make it into the final version of the Regulation (discussed below). However, taking into account that the right to data protection belongs to the child and not to their representative (who is merely appointed to exercise them), legal incapacity until the age of 18 can be easily seen as overprotective. Following the requirements of the UN CRC, children should be increasingly consulted on matters relating to them and thus solutions for consent could range from mere consultation with the child, to parallel or joint consent of the child and a parent, or even to the autonomous consent of a mature child.[125] As a result, diverging age thresholds, rarely as high as 18, are explicitly introduced (or tacitly accepted in practice, depending on the Member State) for minors as data subjects while regulating their power to give a valid consent to the data processing operations. A large discrepancy exists with regard to the age, after which minors are legally competent to give their consent.[126] In general, many European countries consider minors ranging from 14 to 16 years to be competent to consent to the processing of their data. However, the precise question of whether a particular minor is competent and, more importantly, has given valid consent in a particular context might still depend on all the

[123] Arlene Skolnick, 'The Limits of Childhood: Conceptions of Child Development and Social Context' (1975) 39 Law and Contemporary Problems, 38.

[124] Rachel Hodgkin and Peter Newell, *Implementation handbook for the Convention on the Rights of the Child*, (Unicef, 2002), 1.

[125] Article 29 Working Party (A29WP), 'Opinion 2/2009 on the protection of children's personal data (general guidelines and the special case of schools) WP 160', 11 February 2009.

[126] Terri Dowty and Douwe Korff, 'Protecting the virtual child – the law and children's consent to sharing personal data' (Study prepared for arCh - action on rights for Children- and the Nuffield Foundation), 2009 <http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf> accessed 1 March 2017.

circumstances, including both subjective matters such as the maturity of the minor and more objective matters such as whether the matter for which consent was given was in the direct interest of the minor or not, and indeed whether the parents were, or should have been involved.[127]

2.2.2. Three distinct national choices

The lack of harmonised general rules on children's data processing and consent, opened the door for individual EU member states to nationally set their age limits at which parental consent is required and foresee how valid consent from minors should be obtained. Legal regulations or solely existing opinions and best practices on the age threshold for a valid consent of a minor notably differ across the EU Member States and the legal capacity to consent to data processing operations varies not only in different jurisdictions but also across sectors, like research[128] or advertising[129].

The broad range of diverging practices among the EU Member States in the area of data protection may be divided into three groups in relation to the method and interpretation of the exact age threshold enabling minors to consent to their data protection.

2.2.2.1. An objective bright-line approach

A few Member States explicitly state in their national data protection law the exact age threshold from which minors are treated as legally competent to act as data subjects on their behalf. This regulatory choice can be called an objective bright-line rule.[130] In Spain, the data protection law contains specific provisions on the consent for the processing of data on minors.[131] According to Article 13 of the Spanish Personal Data Protection Law, data pertaining to data subjects over 14 years of age may be processed with their consent, except in cases when the law requires the assistance of parents or guardians. The same article also forbids the collection of data from minors regarding members of their family or its members' characteristics, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refers. The exception is data regarding the identity and address of the father, mother or guardian which may be collected for the sole purpose of obtaining their consent. The Spanish

[127] Ibid.

[128] As to the legal requirements and procedures for involving children in research, including in particular procedures of ethics approval and informed consent of children and their parents for all EU Member States see the Fundamental Rights Agency, 'Legal requirements and ethical codes of conduct of child participation in research in EU Members States', 2014 <http://fra.europa.eu/en/theme/rights-child/child-participation-in-research#80> accessed 10 April 2017.

[129] For example, UK's Advertising Standard Authority, The UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing, Edition 12, <https://www.asa.org.uk/asset/47EB51E7%2D028D%2D4509%2DAB3C0F4822C9A3C4/> accessed 10 April 2017 (defines a child as an individual under 16).

[130] Lina Jasmontaite and Paul de Hert, 'The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet', (2015) 5(1) *International Data Privacy Law 20.*

[131] Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

law also underlines the responsibility of the data controller for the setting up of the verification procedures that guarantee the age of the minor and the authenticity of the parental consent.

Similarly, although stipulated in less detail, the data protection law in the Netherlands states that "(I)n the case that the data subjects are minors and have not yet reached the age of sixteen, or have been placed under legal restraint or the care of a mentor, instead of the consent of the data subjects, that of their legal representative is required. The data subjects or their legal representative may withdraw consent at any time" (Article 5 Dutch Data Protection Law).[132] The Dutch Data Protection Authority specified the obligation to obtain valid consent from those under the age of 16 online in its guidelines entitled "Publication of personal data on the Internet" which was adopted in 2007.[133] The Dutch data protection authority does not specify or recommend concrete methods for obtaining the consent of a minor's parents or legal representatives, but underlines the general principle that the data controller must be able to demonstrate that consent has been obtained, alternatively consent is void and any subsequent processing of the personal data online is unlawful. It also points to a social responsibility of the website owners and network environments aimed at those under the age of sixteen to explain the rights and obligations of their users in a clear and understandable language.

Additionally in Hungary, Section 6 sub-section 3 of the Hungarian Privacy Act[134] clearly states that "(T)he statement of consent of minors over the age of sixteen shall be considered valid without the permission or subsequent approval of their legal representative".

Finally, the UK Data Protection Act 1998, albeit not directly referring to the age of consent, has a special section on the exercise of rights in Scotland by children which states: "where a question falls to be determined in Scotland as to the legal capacity of a person under the age of sixteen years to exercise any right conferred by any provision of this Act, that person shall be taken to have that capacity where he has a general understanding of what it means to exercise that right." It further specifies: "a person of twelve years of age or more shall be presumed to be of sufficient age and maturity to have such understanding" [135].

All four of the above-mentioned EU countries introduced the age limit for consent of minors as a general requirements, without making a specific reference to consent in the online environment. Thus, this requirement is equally applicable to data processing online.

2.2.2.2. "Regulation by analogy" approach

Some other Member States chose the "regulation by analogy" model and invoke civil law provisions establishing when a person becomes fully competent to acquire and assume rights and obligations and apply them to the area of data protection. For example, in Lithuania

[132] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

[133] Dutch Data Protection Authority, 'Publication of personal data on the Internet' (guidelines), December 2007 <https://cbpweb.nl/sites/default/files/downloads/mijn_privacy/en_20071108_richtsnoeren_internet.pdf> accessed 8 May 2016 sub-section 4.1.

[134] Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

[135] Section 66 of the Data Protection Act 1998. For the explanation of this, rather confusing, section see Terri Dowty and Douwe Korff, 'Protecting the virtual child – the law and children's consent to sharing personal data' (Study prepared for arCh - action on rights for Children- and the Nuffield Foundation), 2009, 15-16.

children can be considered as competent from 14 years old, as from that age they enjoy partial rights and are allowed to carry out basic legal acts without the consent of their representatives. Consequently they are also allowed to consent to some basic personal data processing operations.[136]

2.2.2.3. Subjective capacity-based approach

Many Member States seem to have no bright-line specific provision or rely on the legal capacity of agents in other branches of law but instead assess the concrete situation on case-by-case basis applying the general criteria of the best interest of the child, level of moral and psychological development, the capacity to understand the consequences of giving consent and evaluating specific circumstances (the age of the child, the purpose of data processing, type of personal data involved,[137] etc). Such an evaluation of the capacity of the data subject is a subjective and context-specific test rather than one that is universally applicable, but assumption-based exemplar age thresholds are normally set in case law, legal doctrine or guidelines from the data protection authorities. This choice can be called the subjective capacity test. For example, in the UK, there is a general presumption that no assumptions about an individual under 16 can be made as they lack legal capacity. Although there is no case law about children's capacity to consent to data processing, the existing case law developed some guidance on the situations in which children can give consent to a medical treatment or legal representation.[138] The seminal case on the matter is *Gillick v. West Norfolk and Wisbech Area Health Authority*. This case developed guidelines under which a doctor can lawfully provide contraception to a girl under 16 years old without informing her parents. It established a principle that children under 16 can sometimes give their consent to certain things, but there is no fixed age when one can presume the competence of a child.[139] In the UK, the Data Protection Act 1998 does not deal with the issue of obtaining consent from children. The main document providing guidance with regard to data collection online is issued by the UK Information Commissioner's Office (UK ICO) through the Personal Information online code of practice adopted in 2010. The code states that "assessing understanding, rather than merely determining age, is the key to ensuring that personal data about children is collected and used fairly". When services are directed at children, the UK ICO advises: to determine the level of understanding of the child rather than only the age; to require parental consent for children under the age of 12; to collect information in a way that children understand and to which parents are not likely to object. When the information obtained from the child is relatively speaking of less importance or sensitivity (such as name), then simple notification of parents via email is enough, whereas when a photograph of the child is being processed then something more akin

[136] M Macenaite and others, Vaiku privatumo apsauga internete (Lithuanian Consumer Institute, Vilnius 2011) 33, 69.

[137] In Austria, for example, there are no legal restrictions or case law, although the age of 14 is usually taken as the cut-off point below which consent is required, except for the processing of sensitive data, for which parental consent is required for all minors.

[138] Terri Dowty and Douwe Korff, 'Protecting the virtual child – the law and children's consent to sharing personal data' (Study prepared for arCh - action on rights for Children- and the Nuffield Foundation), 2009 <http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf> accessed 1 March 2017, 8.

[139] LSE Working Group on Consumer Consent, 'From legitimacy to informed consent: mapping best practices and identifying risks' (2009) <http://www.lse.ac.uk/management/documents/research/research-initiatives/Report-on-Online-Consent.pdf> accessed 3 March 2017, 54-55.

to verifiable parental consent is necessary. In Belgium the issue of minors' consent has been addressed in an Advice issued by the Belgian Data Protection Authority.[140] The Advice states that even though under Belgian law, the age of maturity is 18 years, the gradual development of minors and the need for more independence with growth should be acknowledged, especially in adolescence, between the ages of 13 and 16 years. When a child is not mature enough to be able to understand the implications of the given consent parental consent is necessary. For those younger than 13 or 14 consent is required in all cases, however in complicated cases parental consent is also mandatory for children younger than 15 years. Parental consent should also be gained when sensitive data are collected from those under 16, and in all cases when data processing is not in the interest of the child.

At a European level, the approach is similar to the majority of the national jurisdictions described in the third group. The Article 29 Working Party in the Opinion dedicated to the protection of children's privacy,[141] took a similarly flexible approach and did not set precise age limits at which parental consent is required. Instead, it underlined the importance of the maturity of a child and complexity of the data processing at hand. For instance, the Article 29 Working Party believed that data collection from an 8-year-old child for the purpose of sending a free magazine or newsletter does not require parental consent, while such consent would be necessary for the same child to take part in a live TV show.

3. Consent in EU Data Protection Law

3.1 The concept of consent

The consent of the data subject as a legitimate basis for personal data processing is recognised in the Charter of Fundamental Rights of the European Union (CFR)[142] and further in the Data Protection Directive (Article 7 DPD). The GDPR retains consent of the data subject as one of the grounds for lawful processing of personal data (Article 6(1)(a) GDPR).

The consent of the data subject in the context of the Data Protection Directive is understood as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Article 2(h) DPD). The definition of consent in the GDPR remains very close to the definition of the term in the DPD: "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by

[140] Belgian Privacy Commission, 'Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet' (2002) <http://www.privacycommission.be/nl/docs/Commission/2002/advies_38_2002.pdf > (Dutch); <http://www.privacycommission.be/fr/docs/Commission/2002/avis_38_2002.pdf> (French), accessed 1 March 2017.

[141] Article 29 Data Protection Working Party, 'Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160', 11 February 2009.

[142] The Charter of Fundamental Rights of the European Union, which came into force on 1 December 2009, besides a right to private life (Article 7), recognised the protection of personal data as a separate right under its Article 8. Article 8 of the Charter safeguards the protection of personal data and Article 8 Part 2 stresses the processing of personal data on the basis of consent or other legitimate grounds by stating: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*"

a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 4(11) GDPR).

The Article 29 Working Party closely examined the concept of consent in the DPD in its opinion on the definition of consent[143], specifying and examining the criteria for the consent of the data subject to be valid. According to the Article 29 Working Party, the consent must be (a) an indication of the wishes of the data subject… signifying…, (b) freely given, (c) specific, and (d) informed. These elements will now be briefly discussed as they remain identical to the definition of consent contained in the GDPR and will be then followed by a short discussion of the "unambiguous" qualification.

a) Indication of the wishes of the data subject

An essential element in deciding if the data subject consents to a specific processing operation is the examination of whether there is a clear indication of the wishes of the data subject. The GDPR clarifies in the definition of consent that data subject should indicate his wishes using a statement or a clear affirmative action (Article 4(11) GDPR). Therefore consent cannot be inferred from the absolute silence of the data subject. Similarly pre-ticked boxes or lack of any action on behalf of the data subject does not constitute consent (Recital 32 GDPR). Recital 32 GDPR clarifies that an indication of the wishes of the data subject can be provided "by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. […] If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided" (Recital 32 GDPR).

b) Freely given consent

There are various influences that can be exercised on data subjects in order to manipulate their decision to agree to the processing of their personal data. However, not every exercise of external pressure leads to invalidation of consent. The consent of the data subject is still freely given when positive pressure is exercised, while the exercise of any kind of negative pressure renders the consent invalid. Recital 42 GDPR clearly summarises that "[c]onsent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment." The GDPR clearly stipulates that in order to assess whether consent in freely given "utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of the contract" (Article 7(4) GDPR). Similarly consent will not be deemed to be freely given if this relates to more than one data processing operation and it is not possible to separate out consent on the basis of each individual data processing operation (Recital 43). Moreover recital 43 clarifies that consent should not be considered as freely given and the processing of personal data should not rely on it when there is clear imbalance between the data subject and the data controller "in

[143] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent, WP 187', 13 July 2011.

particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation." (Recital 43 GDPR).

c) Informed consent

The provision of adequate information to the data subject is context-related. The types and amount of information should be decided on a case-by-case basis in the light of the fairness principle. That being said, the information that is specified in Article 13 GDPR should be provided to data subjects irrespective of the circumstances as complemented by any other information that is required in order to properly informed the data subjects vis-à-vis the specific circumstances of the processing. The information should be easily accessible, easy to understand and should be provided in an intelligible form (Recital 39 GDPR). Recital 39 GDPR provides a short description of the transparency principle and indicates that this in particular concerns the provision of "information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed" (Recital 39 GDPR). In the context of the novelties introduced in the GDPR where risk plays a prominent role in the handling of personal data, the GDPR requires that specific information is provided to the data subjects with regard to the risks, conditions of processing, relevant safeguards in place as well as the rights of the data subjects in relation to the processing of personal data (Recital 39 GDPR). In particular the provision of information to children, in light of the fairness principle, should be adapted to children, in order to make it easy for them to understand what information is collected about them and for what purposes it will be used.[144]

d) Specificity of consent

The GDPR provides that the consent of the data subject should be specific. The requirement for specificity relates to all circumstances surrounding the processing of the personal data for which the consent is been sought. The specification of the information that is provided to the data subject is an intrinsic element of the requirement for informed consent. However, the element that the consent has to be specific also relates to the degree of specificity it has to ascertain. Valid consent requires the explicit specification of the aimed legitimate purposes (recital 39 GDPR). It is unclear to what extent clearly specified consent, covering for instance multiple purposes, could be invalid. On this point the GDPR clarified that multiple processing operations that are carried out for the same purpose(s) can be covered under one consent (Recital 32 GDPR). Similarly, when a processing operation is carried out for multiple purposes, then consent should be provided for all of them (Recital 32 GDPR).

The definition of consent in the GDPR includes the additional requirement that consent needs to be unambiguous, a qualification that was required only in two instances under the Data Protection Directive: when consent was the ground for legitimate processing of personal data (Article 7(a) DPD) and in the context of transfers of data to third countries (Article 26(1) DPD).

[144] Article 29 Working Party, 'Opinion 15/2011 on the definition of consent WP 187', 13 July, 2011, 37; Recital 58 of the GDPR: "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand."

Several Member States, such as Germany and the United Kingdom, chose not to incorporate the qualification of "unambiguously given" consent in their national data protection legislation when transposing the Data Protection Directive. Kosta claims that "The additional condition that the consent should be given "unambiguously" does not add any real value to the way how consent should be interpreted. A consent given "ambiguously" would amount to an unclear indication of the wishes of the data subject for processing of his personal data and would not qualify as valid consent."[145] The European Commission in its Proposal for the General Data Protection Regulation introduced the element that consent has to be "explicit" in the definition of the term[146], a proposal that was also welcomed by the European Parliament in its first reading.[147] The Council of the European Union in its first reading did not include either the qualification of unambiguous or explicit consent. However, as already discussed, the final version of the GDPR, which resulted from the Trialogue debates, included a qualification of unambiguous consent in the definition of the term, despite the controversy as to whether this qualification has any actual value.

3.2 Special conditions for consent

In Article 7 the GDPR sets out specific conditions with regard to the provision of consent that are also of high relevance in the context of the consent of minors. The GDPR clarifies that the data controller must be able to demonstrate that the consent of the data subject has been provided for specified purposes (Article 7(1) GDPR). As the data controllers will be responsible to prove that the consent of the data subject was provided in a valid way for a specific data processing operation, they should also use reliable means in order to obtain the consent, taking into account the sensitivity of each specific data processing operation.[148]

The GDPR also introduces the rule that when data subject consent is provided as part of a written declaration that concerns another matter, then the request for consent has to be presented in a clearly distinguishable form from the other elements of that written declaration in an intelligible and easily accessible form, using clear and plain language (Article 7(2) GDPR). This new rule is already to be found in Germany, where the German Federal Court of Justice published a decision on the "Payback" case, according to which it was sufficient that the clause on the consent to the processing of personal data was clearly highlighted and the data subject was given the opportunity to object to such processing.[149] The clause on consent to data processing should not be simply part of the general terms and conditions of a contract,

[145] Eleni Kosta, *Consent in European data protection law* (Brill/Martinus Nijhoff Publishers, 2013), 235.
[146] Commission (EC), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final (Draft Data Protection Regulation), 25 January 2012.
[147] European Parliament (EP), Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading), 12 March 2014.
[148] European Data Protection Supervisor, 'Opinion on the data protection reform package', 7 March 2012, para. 129.
[149] Bundesgerichtshof (GERMBGH - German Federal court of Justice), Decision of 16 July 2008, Az: VIII ZR 348/06 ("Payback"), MMR 2008, 731.

without any special highlighting,[150] nor can it be included in the fine print of the contract, as the data subject can easily overlook it.[151] According to Article 7(3) GDPR the data subject has the right to withdraw his consent at any time; however the withdrawal does not affect the lawfulness of the processing that was based on consent before the withdrawal (Article 7(3) GDPR).

The application of the general requirements for a valid consent (as mentioned above) is complex. However, this complexity is further intensified in the context of the consent of minors in the online environment. For example, the requirement of a freely given consent becomes more complicated in circumstances where children could give their consent without the involvement or knowledge of parents and this is particularly problematic given that very often their choices may be manipulated and vulnerabilities exploited for commercial purposes due to their increasing spending power.[152] Fulfilling the requirements for informed consent is particularly challenging in case of minors, as their level of understanding and ability to foresee possible consequences differs from adults. Although the use of privacy policies is a common practice and many of them formally follow legal requirements regarding the obligatory information, it is doubtful whether they achieve their goal.[153] However, even with extensive information available and especially given the complexity of profiling techniques and big data analytics that are difficult even for adults to comprehend, many minors would still be unable to properly measure the significance of their consent as regards the impact on their privacy and personal autonomy. Many privacy policies are long, hard to find and navigate, written in complicated language and are beyond the capacity of an average adult to understand.[154]

[150] Helmut Redeker, 'Teil 12 Internetverträge' in Thomas Hoeren and Ulrich Sieber (eds), *Handbuch Multimedia-Recht - Rechtsfra-gen des elektronischen Geschäftsverkehrs* (Ergänzungslieferung) (2010), para. 111.

[151] Bundesgerichtshof (BGH - German Federal Court of Justice), Decision of 16 July 2008, AZ: VIII ZR 348/06 ("Pay-back"), MMR 2008, 733; Peter Gola and Rudolf Schomerus BDSG - Bundesdatenschutzgesetz, Kommentar (8th ed. 2005) Section 4a, para. 14; Spiros Simitis (ed.), Kommentar zum Bundesdatenschutzgesetz (5th ed. 2003), Section 4a, para. 40; Thomas Hoeren, 'Die Einwilligung in Direktmarketing unter datenschutzrechtlichen Aspekten' (2010) Zeitschrift für die An-waltspraxis, 434.

[152] Kathryn C. Montgomery, 'Youth and surveillance in the Facebook era' (2015) 39(9) Telecommunications Policy 771; Valerie Steeves and Ian Kerr, 'Virtual playgrounds and buddybots: a data-minefield for tinys & tweeneys', Panopticon, 15th Annual Conference on Computers, Freedom & Privacy, Keeping an Eye on the Panopticon: Workshop on Vanishing Anonymity, Seattle, April 12, 2005.

[153] Patrick Van Eecke and Maarten Truyens, 'Privacy and Social Networks' (2010) 26 Computer Law &Security Review, 542.

[154] UK Children's Commissioner, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (January 2017) <http://www.childrenscommissioner.gov.uk/sites/default/files/publications/Growing%20Up%20Digital%20Taskforce%20Report%20January%202017_0.pdf> accessed 9 April 2017; Jacquelyn Burkell, Valerie Steeves and Anca Micheti, 'Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand' (report), March 2007 <http://www.idtrail.org/content/view/684/42/> acessed 10 April 2017, 1-2. On privacy policies in social networks in general see, Joseph Bonneau and Sören Preibusch, 'The Privacy Jungle: On the Market for Data Protection in Social Networks' (The Eighth Workshop on the Economics of Information Security, London, 24 June 2009) <http://www.jbonneau.com/doc/BP09-WEIS-privacy_jungle.pdf>, accessed 9 March 2017.

4. Legislative history of Article 8

The GDPR devotes a specific Article to the processing of the personal data of children which pays special attention to issues related to consent. The legislative history of Article 8 of the GDPR is thin. It seems that the majority of the debates during the GDPR legislative process focused more around articles with a direct economic impact on data controllers' activities and the Digital Single Market, such as the one-stop-shop mechanism or profiling, rather than protection of vulnerable data subjects. Article 8 witnessed sporadic renewals of interest during the debates and clearly lacked well-reasoned justifications and evidence before adoption. Nevertheless, this section aims to chronologically delve into the positions of the EU institutions involved in the legislative process and the changes they proposed to Article 8.

4.1. Commission proposal

A first unofficial version of the EC Proposal for the GDPR[155] was leaked online in December 2011 by StateWatch. In this text a child was defined as any person under 18 years (Article 3 Part 18). This definition echoed the understanding of childhood in accordance with the UN CRC. That version of the GDPR did not contain any specific articles on the processing of the personal data of a child. Instead, Paragraph 6 of Article 7 which specified the conditions for consent established that the consent of a child is only valid when given or authorized by the child's parent or custodian. This approach demonstrates that at the beginning of the data protection reform process the European Commission (EC) had no intention of differentiating between digital and offline consent and aimed at protecting equally everyone below the age of 18. The same is confirmed in the questions that the EC posed to the key stakeholders in the targeted consultation meetings in 2010, asking if "a harmonized age limit of 18 years in line with Article 1 of the UN Convention on the Rights of the Child" should be adopted to better protect the personal data of minors.[156]

The Proposal for a General Data Protection Regulation[157], officially presented by the European Commission on 25 January 2012, retained the definition of a child as any person below the age of 18 years (EC proposal GDPR). However, just before publishing the Proposal (during the Commission inter-service consultation process) an amendment to the article on consent was

[155] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) Version 56 (29/11/2011), <http://statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf > accessed 10 April 2017.

[156] Commission (EC), 'Stakeholders' Consultations "Future of data protection"' (background paper) http://ec.europa.eu/justice/news/events/data_protection_regulatory_framework/background_paper_en.pdf accessed 10 April 2017, question 4.

[157] Commission (EC), Draft Data Protection Regulation, COM (2012) 11 final.

unexpectedly introduced and a new Article on the processing of the personal data of a child was added to the GDPR.

In relation to the offering of information society services directly to children, the age limit at which the personal data of a child cannot be processed without parental consent was lowered to 13 years (Article 8 Part 1). The European Data Protection Supervisor (EDPS) found this approach "reasonable"[158], while the Article 29 Working Party suggested that the scope of application of this provision was broadened in order to cover other areas where the processing of personal data of children is taking place, outside the provision of information society services.[159] According to the EC proposal the EC would have retained the power to specify concrete methods to obtain valid consent for the processing of the personal data of children[160] and to publish delegated acts specifying the criteria and the conditions under which the consent of a child can be provided in a valid way[161]. The EDPS, however, expressed concerns with such delegated acts that would specify criteria and requirements for the methods in order to obtain verifiable consent in relation to the specific measures which the Commission might envisage for micro, small and medium-size enterprises.[162]

4.2. European Parliament first reading

The Commission's draft GDPR proposal was subject to intensive discussions and lobbying at the European Parliament. In the Civil Liberties, Justice, and Home Affairs (LIBE) Committee alone 3999 amendments to the GDPR were proposed. On the 21st of October 2013, the LIBE Committee adopted the amendments to the EC proposed Regulation, including amendments to Article 8. The amendments proposed by the LIBE Committee were almost unanimously approved in the first reading of the European Parliament on 12 March 2014.[163]

Despite the amount of amendments registered, the discussions at the European Parliament (EP) did not lead to major substantive changes for Article 8 but instead only to small modifications. The EP, in essence, avoided questioning the necessity of having parental control through consent or indeed adopting a more nuanced version. It also refrained from publicly debating the reason of limiting the parental consent requirement to children below the age of 13 or questioning the burden and ineffectiveness of the parental consent mechanisms. The EP mainly introduced a specific information obligation requiring that information be "provided in a clear language appropriate to the intended audience" (Article 8(1a) EP first reading). It also deleted the authority of the EC to adopt implementing acts with standard forms for verifiable consent. Instead it designated the European Data Protection Board as responsible to issue guidelines,

[158] European Data Protection Supervisor, 'Opinion on the data protection reform package', para. 128.
[159] Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposals WP191', 23 March 2012, 13.
[160] Article 8(4) and Recital 130 draft Data Protection Regulation.
[161] Article 8(3) and Recital 129 draft Data Protection Regulation.
[162] European Data Protection Supervisor, 'Opinion on the data protection reform package', para. 81.
[163] European Parliament, Legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012), 12 March 2014.

recommendations and best practices on how verifiable consent can be obtain or for verifying consent (Article 8(3)3).

However, there were amendments that were tabled in relation to these issues but these were not included into the final text. A group of Parliament members (MEPs) proposed to specifically underline that the protection of children is particularly important in social networks.[164] Other such amendments highlighted that "the industry should take its shared responsibility to come up with innovative solutions, products and services in order to increase the safeguards on protection of personal data, in particular for children, for example through codes of conducts and monitoring mechanisms"[165].

One group of the MEPs proposed to delete Article 8 from the text of the GDPR.[166] The age of a child was questioned by 5 MEPs who proposed to raise the age limit for parental consent from 14 to 15 or 16 years.[167] One MEP suggested to increase the age limit up to 18, but to limit the scope of application (exempt services that "are particularly appropriate and suitable for a child and have been notified and are controlled by the relevant national authorities" from consent requirement) and to accept unreliable consent methods (parents' consent via email).[168]

Notwithstanding the amendments proposed by a number of MEPs, the EP in its first reading made only the following changes. First, it expanded the scope of application of Article 8 and imposed the obligation to obtain parental consent to data controllers processing children's data in the offline world, when offering "goods or services" directly to children rather than "information society services". In such a way, the EP followed the suggestion of the Article 29 Working Party to cover other areas where the processing of the personal data of children is taking place, outside the provision of information society services.[169] Second, the EP required data controllers to give information to children, parents and legal guardians in a clear, audience-appropriate language. As a result, the European Parliament amendments strengthened consent as an informed indication of wishes, in particular in respect to children.[170] A similar provision already existed in the EC proposal (Article 11) but was formulated in general terms and applicable to all data subjects. Third, the EP modified Recital 38 (previously Recital 29) by deleting a reference to the UN Convention on the Rights of the Child as a document from which the definition to determine when an individual is a child should be taken. This deletion did not substantially change anything, as the definition of a child as an individual under 18 years of age still remained in Article 4(18).

---

[164] Committee on Civil Liberties, Justice and Home Affairs (LIBE), Amendments (1) 351 – 601, 2012/0011(COD), 4 March 2013, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2F%2FEP%2F%2FNONSGML%2BCOMPARL%2BPE-504.340%2B01%2BDOC%2BPDF%2BV0%2F%2FEN > accessed 1 March 2017, Amendment 426 by Marian Harkin and Seán Kelly, and Amendment 427 by Sabine Verheyen et al.

[165] Ibid., Amendment 521 by Anna Maria Corazza Bildt and Carlos Coelho.

[166] LIBE, Amendments (3) 886-1188, 2012/0011(COD), 4 March 2013, < http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/am/928/928600/928600en.pdf > accessed 10 April 2017, Amendment 1005 by Timothy Kirkhope on behalf of the ECR Group.

[167] Ibid., Amendment 1006 by Csaba Sógo (the age of 14 years), Amendment 1008 by Manfred Weber (the age of 15 years), Amendment 1009 by Birgit Sippel, Petra Kammerevert and Josef Weidenholz (the age of 16 years), Amendment 1012 by Jean Pierre Audy, Seán Kelly, (the age of 15 years).

[168] Ibid., Amendments 1014 and 1019 by Axel Voss.

[169] Article 29 Data Protection Working Party, 'Opinion 01/2012 on the data protection reform proposals (WP191)', 13.

[170] LIBE, Compromise Amendments to the GDPR, A7-0402/2013, 21 October 2013, Article 8 para 1a.

The EP also added an emphasis on grounds other than consent for the lawful processing of the personal data of children: "other grounds of lawful processing such as grounds of public interest should remain applicable, such as for processing in the context of preventive or counselling services offered directly to a child."[171] This shows that the MEPs realised that certain services are created for children who seek help and must be used without their parents' consent, especially in situations where their parents might be closely linked to the problem, such as online-chats for victims of sexual abuse.[172] In other cases, when the interest of parents and children may not coincide consent may also not be the best ground for lawful data processing. This provision partly follows the suggestion of the EP Legal services and Internal Market and Consumer Protection committees which proposed exceptions to the parental consent rule in case of health data processing and social care.[173] The justification was that "in the context of health and social care authorisation from a child's parent or guardian should not be necessary where the child has the competence to make a decision for him or herself. In Child Protection Cases it is not always in the interests of the data subject for their parent or guardian to have access to their data, and this needs to be reflected in the legislation."[174]

A similar amendment was tabled by two MEPs who proposed to adopt an exemption for parental consent in the context of health and social care where the child has the maturity and competence to make a decision on their own.[175] It was stressed, that in the UK, for example, a person of 12 years is presumed to be old and mature enough to exercise the right to decide who else can access their health records.

Noteworthy here is a sliding scale approach to consent proposed by the Legal service of the EP. The proposal took a risk-based approach and recognised various possible forms of consent instead of subjecting consent to a single rule. It stated that "the appropriate form for obtaining consent should be based on any risk posed to the child by the amount of data, its type and the nature of the processing".[176] This proposal was in line with the approach of the Article 29 Working Party.[177] The Article 29 Working Party proposed that the mechanism that would be used for age verification in the online environment each time should depend on various factors relating to the specific data processing operation, such as the types of personal data that will be processed, the purposes for which they will be processed, eventual risks arising from the processing etc.[178]

---

[171] EP Resolution (n 67), Recital 29.

[172] LIBE Amendments (3) 886-1188 (n 70), Amendment 1021 by Birgit Sippel, Petra Kammerevert and Josef Weidenholze.

[173] EP, Opinion of the Committee on Legal Affairs, Amendment 56, 25 March 2013, Opinion of the Committee on the Internal Market and Consumer Protection, Amendment 89, 28 January 2013, <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN#title6> accessed 10 April 2017 (states that the authorisation from a child's parent or guardian should not be necessary "where the processing of personal data of a child concerns health data and where the Member State law in the field of health and social care prioritises the competence of an individual over physical age").

[174] Ibid.

[175] LIBE Amendments (3) 886-1188 (note 70), Amendment 1030 by Claude Moraes and Glenis Willmot.

[176] EP, Opinion of the Committee on Legal Affairs, Amendment 55, 25 March 2013, <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0402&language=EN#title6> accessed 10 April 2017.

[177] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent, WP 187', 13 July 2011, 28.

[178] Ibid.

4.3. Council of the European Union drafts

The most heated debates on the future of Article 8 of the General Data Protection Regulation took place in the Council of the EU. While the European Parliament proposed only revisions to the existing text of the European Commission focusing on the scope of its application, in the Council of the EU substantial debates among the Member States arose around the actual necessity to include any provisions on minors' consent in the GDPR.[179] The drafts of the GDPR published by two different presidencies contain evidence of debates that took place among Member States around article 8 of the GDPR. A revised version of the draft GDPR published by the Greek Presidency on 30 June 2014, reveals that Member States had opposing opinions on the issue.[180] Seven Member States (Czech Republic, Germany, Austria, Sweden, Slovenia, Portugal, UK) held a scrutiny reservation and two countries (Czech Republic and Slovenia) wished Article 8 deleted. Norway[181] proposed in line with its national data protection law[182] the inclusion of a general provision prohibiting the processing of the personal data relating to children in a manner that is contrary to the child's best interest, instead of a specific article on children's consent. Such a provision, it claimed, would allow broader protection as the supervisory authorities would be able to intervene also in cases where, for example, "adults publish personal data about children on the Internet in a manner which may prove to be problematic for the child". Three Member States (Germany, Slovenia and Romania) suggested raising the age limit for consent from 13 to 14 years.[183]

The draft published by the Latvian Presidency of the Council[184] on 11 June 2015 was the basis for the General Approach of the Council on the GDPR. It demonstrated the crystallisation of three diverging views among Member States in relation to article 8. Now more Member States

[179] Council of the European Union, Note from Presidency to JHA Counsellors meeting (DAPIX) - Chapter II, 17072/3/14 REV 3, 26 February 2015, <http://data.consilium.europa.eu/doc/document/ST-17072-2014-REV-3/en/pdf> accessed 10 April 2017.

[180] Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection, 11028/14, 30 June 2014, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011028%202014%20INIT> accessed 10 April 2017.

[181] Norway, although not being an EU country, participated in the debate on the GDPR as it will be applicable to Norway as part of the European Economic Area (EEA) together with Iceland and Liechtenstein.

[182] Norway on 20 April 2012 (Act of 20 April 2012 no. 18., effective 20 April 2012 under Royal Decree 20 April 2012 no. 335) amended its Personal Data Protection Act and among other changes included a provision which strengthens the protection of children's privacy beyond specific reference to their consent. Under the section 11, one of the basic requirements to process personal data, such as explicit purpose, data adequacy, relevancy is the requirement tailored to children as data subjects (i.e. "Personal data relating to children shall not be processed in a manner that is indefensible in respect of the best interests of the child.").

[183] Several delegations (Germany, France, Hungary, Luxembourg, Latvia, Romania, Slovenia) questioned the age of consent being set at 13 years. European Commission clarified that the choice was based "on an assessment of existing standards, in particular in the US relevant legislation (COPPA)". Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection, 11028/14, 30 June 2014, 87–88.

[184] Council of the European Union, Note from Presidency to the Council, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) - Preparation of a general approach 9565/15, 11 June 2015, <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf> accessed 10 April 2017.

voiced a preference to have Article 8 deleted (Czech Republic, Malta, Spain, Slovenia and UK). Potential reasons of their preference to abandon the article relate to the difficulties to unanimously define a child in different EU countries and practical challenges relating to age verification and content obtaining mechanisms.

A larger group of Member States took a middle ground position as they expressed understanding of the merit and would have liked to see a provision on child protection in some form (Austria, Belgium, Cyprus, Germany, Greece, Hungary, Ireland, Italy and Romania).[185] The third group of states took a different turn and instead of strengthening and clarifying parental consent, it proposed adding a limitation on certain data gathering and processing practices in relation to minors (profiling and marketing). France, supported by Estonia, Denmark, Sweden and Poland, suggested deleting Article 8 and instead inserting a particular provision for children when the Articles of the data subjects' rights were discussed, for example in Article 20 on profiling.

The Council draft from the 11th of June 2015 recognised the need for the special protection of children especially in relation to "the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of child data when using services offered directly to a child" (Recital 29).[186] However, the definition of a child as any person below the age of 18 years was deleted from the list of definitions. The Council changed back the scope of Article 8 to focus on children's consent in relation to information society services. In such cases consent must be "given or authorised by the holder of parental responsibility over the child or is given by the child in circumstances where it is treated as valid by Union or Member State law" (Article 8(1)). In this way the Council left it up the Member States to specify the age and the conditions for considering the consent for the processing of personal data of children valid. Moreover, it made it a responsibility of the data controller to verify that consent is provided or authorised by the person that holds parental responsibility over the child (Article 8(1a)). The Council did not include any provision detailing a Commission or European Data Protection Board responsibility to issue guidelines or best practices regarding the obtaining of verifiable consent or on the verification of such consent.

Initially, the Council kept the age limit for parental consent of 13 years that was first introduced by the EC, but a last-minute change raised the age of consent to 16 years.[187] This change generated public outrage, especially among children's rights activists, companies and youths themselves on social media. The provision was interpreted as banning kids from social media and even as being an attack on their human rights (i.e. such as freedom of expression and right to information).[188] In view of the meeting of the Committee of Permanent Representatives on 9

[185] Ibid.
[186] Ibid.
[187] Council of the European Union, Note from Presidency to Permanent Representative Committee, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Preparation for trilogue, 14902/15, 4 December 2015, <http://data.consilium.europa.eu/doc/document/ST-14902-2015-INIT/en/pdf > accessed 10 April 2017.
[188] danah boyd, 'What if social networking becomes 16+?: New battles concerning age of consent emerge in Europe', 18 December 2015, <https://medium.com/bright/what-if-social-media-becomes-16-plus-866557878f7#.si0ns0e2x> accessed 1 April 2017; Sonia Livingstone, 'No more social networking for young teens?', 18 December 2015 <http://blogs.lse.ac.uk/mediapolicyproject/2015/12/18/no-more-social-networking-for-young-teens/> accessed 10 April 2017; Janice Richardson, 'European General Data Protection Regulation draft: the debate', 10 December 2015

December 2015, the final GDPR draft opted for a compromise: the age of consent was set at 16 years, but allowed Member States to set a lower age which could not go below 13 years[189]. Thus, unless otherwise provided by Member State law, controllers must obtain the consent of a parent or guardian when processing the personal data of a child under the age of 16. The only reference to the change in the Council documents that can be found states: "(…) on the conditions applicable to consent given by a child, the co-legislators converged on keeping 'below the age of 16 years' as a common ceiling, while allowing Member States to foresee lower age limits"[190].

On the 15th of June 2015 the Council agreed on a General Approach on the GDPR based on the draft of the 11th of June 2015 and the Presidency of the Council received in this way a negotiating mandate to enter into the trialogue phase with the European Parliament and Commission. The trialogue resulted in a compromise text that was presented on 15th of December 2015[191]. The focus of Article 8 remained on information society services. Aside from the statement that children deserve specific protection of their personal data due to their lower awareness of risks, consequences, safeguards and their rights, additional emphasis was also placed on where such special protections were especially relevant (i.e. when children's data is processed for the purposes of marketing or creating personality or user profiles and the collection of children's data when using services offered directly to a child). The consent of a parent or legal guardian was omitted for preventive or counselling services offered directly to a child.

4.4. Article 8 of the GDPR as adopted

The official position of the Council was adopted on the 6th of April 2016 at first reading[192], it was approved by the EP on the 14th of April 2016 in its second reading[193] and was finally

<https://medium.com/@janicerichardson/european-general-data-protection-regulation-draft-the-debate-8360e9ef5c1#.1jespbnno>, accessed 10 April 2017; Larry Magid, 'Europe's new privacy regulations may limit teens', 17 December 2015 <http://www.connectsafely.org/europes-new-privacy-regulations-may-limit-teens/>, accessed 10 April 2017; Samuel Gibbs, 'Is Europe really going to ban teenagers from Facebook and the internet?', The Guardian, 15 December 2015 <https://www.theguardian.com/technology/2015/dec/15/europe-ban-teenagers-facebook-internet-data-protection-under-16> accessed 10 April 2017.

[189] Council of the European Union, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [first reading] - Analysis of the final compromise text with a view to agreement, 15039/15, 15 December 2015, <http://data.consilium.europa.eu/doc/document/ST-15039-2015-INIT/en/pdf>, accessed 10 April 2017.

[190] Ibid.

[191] Ibid.

[192] Council of the European Union, Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 5419/16, 6 April 2016 <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>, accessed 10 April 2017.

[193] European Parliament, European Parliament legislative resolution of 14 April 2016 on the Council position at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (05419/1/2016 – C8-0140/2016

adopted on the 27th of April 2016[194]. No definition of a child was included in the final text of the GDPR. As a consequence, a number of questions on how the rights, obligations and prohibitions contained in the GDPR (such as the right to erasure, obligations of data protection by design and default, transparent information, prohibition of profiling), related to children should be applied in terms of scope. It remains unclear whether they cover all children under 18 years old or different age limits (e.g. national age limits in analogy with Article 8), should apply. Article 8 retained its focus on the conditions applicable to children's consent in relation to information society services. An information Society Service is understood under the GPDR as "a service as defined in point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council"[195] (Article 4(25) GDPR). The age limit of 16 was set as the rule for consent to the processing of personal data of a child, but this retained the possibility for Member States to use a lower age which could not go below 13 years. Recital 29 was renumbered to Recital 38 without however any substantial changes in its content. For the rest, Article 8 followed the amendments introduced in the draft of the 15th of June 2015, discussed above.

As a consequence, the adopted Article 8 of the GDPR left the existing state-of-the-art essentially unchanged: no coherent and uniform age threshold in the European Digital Market on when children can consent to their data processing themselves and to what extent their consent is valid. The remaining inconsistent age standards across the EU and between the EU and the US, not only undermines much-anticipated harmonisation effect of the GDPR, but also maintains significant challenges for companies that provide international services. Also, as noted by Kress and Nagel, the "possibility to enact deviations could water down the level of protection which is initially awarded by Art. 8 GDPR"[196]. It is unclear whether Member States will act together to unify the age threshold in any way. At the time of writing, there have been discussions on lowering the age of consent to 13 years of age in at least two member states, the UK[197] and Belgium,[198] while the German draft for a new Federal Data Protection Act has retained the threshold of 16 years[199].

– 2012/0011(COD)) (Ordinary legislative procedure: second reading), <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0125+0+DOC+XML+V0//EN> accessed 10 April 2017.

[194] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[195] Directive (EU) 2015/1535 of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services [2015] OJ L 241/1.

[196] Sonja Kress and Daniel Nagel, 'The GDPR and Its Magic Spells Protecting Little Princes and Princesses. Special regulations for the protection of children within the GDPR' (2017) 18(1) Computer Law Review International 6.

[197] James Titcomb, 'Britain opts out of EU law setting social media age of consent at 16', 16 December 2015, <http://www.telegraph.co.uk/technology/internet/12053858/Britain-opts-out-of-EU-law-raising-social-media-age-of-consent-to-16.html>, accessed 3 March 2017.

[198] The Flemish Office of the Children's Rights Commissioner, 'Advies bij General Data Protection Regulation van de EU, pleidooi sociale media vanaf 13 jaar', 2015-2016/09, 22 April 2016, <https://issuu.com/kinderrechten/docs/da6bbfb1-8a02-4d3f-9794-c31c0fd07d7a/1?e=6593254/36333697 >, accessed 3 March 2017.

[199] Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), 18/11325, 24 February 2017 <http://dip21.bundestag.de/dip21/btd/18/113/1811325.pdf>

From a policy making perspective, despite the efforts to promote the rights of the child in the EU policy making, the GDPR provision on the age of consent seems to be opaque, inconsistent and lacking explanations and evidence from the beginning. The European Commission originally did not have a strong position in relation to the protection of the personal data of children but changed its view on the age for parental consent during the revision process without clear justifications. Despite a number of amendments introduced by various members, the European Parliament avoided discussion of Article 8 choosing to focus its attention on other, more digital market related, articles. The Council has substantially deviated from the original EC proposal. It has initially increased the age limit of consent to 16 years and in the last minute of negotiations adopted a flexible approach leaving the decision partially to the Member states. Even more controversially, the EU was given a chance to re-affirm its commitment to protect the rights of the child in the information society, in the ePrivacy Regulation proposed on 10 January 2017[200] which is as a lex specialis to the GDPR (Art. 1 I GDPR and recital 5 of the GDPR). It missed that opportunity, as the ePrivacy regulation neither continues the distinction between adults and children as data subjects nor refers to the specific requirements of Article 8 of the GDPR. Although it might be argued that protection of electronic communications can be generally addressed, a clear reference to the GDPR parental consent requirement would have been welcomed[201] and demonstrate consistency and commitment to the purpose of protecting children online.

5. The US COPPA and parental consent

Introduced more than 15 years ago in the US, the Children's Online Privacy Protection Act (COPPA)[202] is one of the first pieces of legislation adopted to specifically protect the privacy of minors under 13 years of age online. Although not entirely uncontroversial, COPPA "seeks to put parents in control of what information commercial websites collect from their children online".[203] It has been considered by the Federal Trade Commission (FTC), COPPA's primary enforcer, as an effective act protecting children without unduly burdening operators of online services[204], but heavily criticised by others due to its limited scope (children below the age of 13), the burden of parental consent mechanisms for service operators, the possible impact on online anonymity, and the balance between parental and service provider responsibility.[205]

As a general rule, COPPA requires online services that are directed towards children or that have actual knowledge that they have users under 13 (e.g., because the service collects date of

[200] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), Official Journal [2002] OJ L 201/37.

[201] Sonja Kress and Daniel Nagel, 'The GDPR and Its Magic Spells Protecting Little Princes and Princesses. Special regulations for the protection of children within the GDPR' (2017) 18(1) Computer Law Review International 6.

[202] Children's Online Privacy Protection Act 1998, 15 U.S.C. 6501–6505.

[203] FTC, 'Children's Online Privacy Protection Rule: Not Just for Kids' Sites', <https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites> accessed 3 March 2017.

[204] FTC, 'Implementing the Children's Online Privacy Protection Act: A Report to Congress', February 2007, <http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf> accessed 3 March 2017.

[205] Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016), 208 (he provides an overview of critique for COPPA as a privacy measure).

birth) to obtain verifiable parental consent before collecting any personal information. COPPA applies only to commercial service providers and non-profit entities generally are not covered by the parental consent requirement.

Under COPPA, "verifiable parental consent" means that the consent method must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent. The FTC specifies several possible methods of obtaining verifiable consent, if children's personal information is going to be disclosed to third parties (except service providers) or made publicly available online, such as in a chat, profile or similar feature. These include, for example:

- providing a form the parent can print, fill out, sign and post, fax or scan and email back;
- requiring the parent to use a credit card or similar method of payment (such as PayPal) in connection with a monetary transaction (this could include a membership or subscription fee, or simply a charge to cover the processing of the card);
- maintaining a free-phone (toll free) number staffed by trained personnel for parents to call in their consent;
- permitting the parent to connect to trained personnel via video conference; or
- verifying the parent's identity by checking a form of government-issued ID against a database of such information, provided that the ID is deleted promptly after verification is complete.

In cases where the information is not going to be disclosed or made publicly available, an additional method known as "email-plus" is allowed. This method involves the service operator's obtaining consent through the receipt of an email from the parent, plus one further step. Either the service provider can request a postal address, telephone or fax number for the parent and follow up directly with the parent, or it can, after a reasonable delay, send another email to the parent to confirm their consent.

COPPA foresees certain exceptions to the general consent rule. Verifiable consent is not needed when: (1) responding to a one-time request from a child, provided that the child's personal information is deleted after the response is made; (2) collecting personal information in order to send the child periodic communications such as newsletters, provided that the parent is given the opportunity to opt out; (3) where necessary to protect the safety of a child participating in the service; or (4) where necessary to protect the security/integrity of the service, respond to a judicial request or other public investigation.

In practice, most child-directed online services appear to operate under one of the exceptions to COPPA that allows a one-time use, multiple online contact with simply a notice to a parent (and opportunity to opt out), or e-mail plus.[206] This limited use of legal COPPA provisions can

[206] Advertising Education Forum, 'Children's data protection and parental consent: A best practice analysis to inform the EU data protection reform', October 2013 <http://www.aeforum.org/gallery/5248813.pdf> accessed 10 April 2017, 18.

be claimed to demonstrate the reluctance among industry to fully embrace COPPA in their services.

Contrary to the child-specific services, general audience sites and services do not have to obtain parental consent unless they have actual knowledge that their users are under 13. In practice, this means that many general audience services expose themselves to COPPA only if they collect age or date of birth. As a result, for them to avoid having to comply with COPPA (i.e. to avoid acquiring actual knowledge that a user is a child) it is simply sufficient to avoid the collection of the age or the date of birth of users. In contrast, although general audience sites and services do not have an obligation to collect age information, some service providers take precautions by explicitly prohibiting the users under 13 from using the service in the terms and conditions and asking all users to enter their birth date before they can access the service. In accordance with the FTC's suggestion, they ask for the age in a neutral manner, i.e. allowing any birth date to be entered without stating or implying that a user has to be at least 13. If the date given proves users to be under 13, they age gate and block them. In addition, a cookie can be placed on their computer preventing them from simply re-entering false information.

From the 1st of July 2013 the FTC amended COPPA in order to clarify its scope and strengthen protection for children's personal information (i.e. to minimize the collection of personal information from children and create a safer, more secure online experience for them) in light of changes in online technology and the evolving use of such technologies by children since COPPA first went into effect in April 2000.[207] The amendments include modifications to the definitions of operator, personal information, and Web site or online service directed to children. It also updated the requirements set forth in the notice, parental consent, confidentiality and security, and safe harbor provisions, and added a new provision addressing data retention and deletion.

6. Understanding parental consent in practice

As Article 8 of the GDPR is without precedent in Europe, its practical implementation raises many questions, such as to which services the requirement will apply, how child directed services will be delineated, and how consent and age should be verified. These questions will need to be addressed by the national legislators, data protection authorities (DPAs) and the European Data Protection Board (EDPB) where relevant in the future. In this part we will therefore discuss the key uncertainties that merit attention before the GDPR comes into effect.

6.1. Information society services

The general GDPR provisions apply to any service that involves personal data processing, wholly or partly by automated means or when personal data form part of a filing system (Article 2 GDPR). Article 3 explicitly specifies that it applies to free services offered to data subjects

[207] FTC, Children's Online Privacy Protection Rule, Final rule amendments, 78(12) Fed. Reg. 3972, 17 January, 2013.

in the EU by a controller or processor not established in the EU territory.[208] To the contrary, the parental consent requirement, i.e. Article 8 GDPR, has a specific material scope and is applicable to the information society services offered directly to a child. To define the meaning of the specific scope of application of Article 8, the GDPR makes use of the definition of an information society service contained in Directive (EU) 2015/1535 which defines such services as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services" (Point (b) of Article 1(1) Dir. 2015/1535).[209] The notion of "remuneration" under this definition could be interpreted in a very restrictive way, requiring the user to pay for the provided service. However the majority of the services offered in the information society do not directly require remuneration from the users, including free social media, online gaming, entertainment sites, email or instant messaging services. Therefore, the phrase "normally provided for remuneration", should be interpreted broadly. The European Court of Justice has dealt with the concept of remuneration in the context of services offered within the European Union in various cases and has adopted such an interpretation. In Belgium v Humbel the European Court of Justice considered that "the essential characteristic of remuneration […] lies in the fact that it constitutes consideration for the service in question and is normally agreed upon between the provider and the recipient of the service"[210]. It is not the recipient who necessarily gives the remuneration; the critical element is that the remuneration is given to the provider of the service. Indeed in Bond van Adverteerders v Netherlands, the Court of Justice of the European Union found that the remuneration does not need to come from the recipient of the service (i.e. in this case the viewer), instead it suffices that the remuneration comes from another party, such as an advertiser.[211] The Court of Justice of the European Union has further ruled that a service can be considered as provided for remuneration even in cases where the provider is a non-profit organisation, when there is an "element of chance" inherent in the return or when the service

[208] Article 3 states: "Territorial scope:
1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
    a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
    b. the monitoring of their behaviour as far as their behaviour takes place within the Union."

[209] In contrast, the US COPPA does not mention the distinction between free and paid online services, and applies to operators of child-directed websites and online services collecting personal information, broadly covering "any service available over the Internet, or that connects to the Internet or a wide-area network". According to the FTC, "examples of online services include services that allow users to play network-connected games, engage in social networking activities, purchase goods or services online, receive online advertisements, or interact with other online content or services. Mobile applications that connect to the Internet, Internet-enabled gaming platforms, voice-over-Internet protocol services, and Internet-enabled location-based services also are online services covered by COPPA". See FTC, 'Complying with COPPA: Frequently Asked Questions', Section A. Question 9. <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Audience>" accessed 3 March 2017.

[210] C-263/86 *Belgian State v René Humbel and Marie-Thérèse Edel (Belgium v Humbel)* [1988] ECR 5365, para. 17.

[211] C-352/85 *Bond van Adverteerders v Netherlands State* [1988] ECR 2085. Paul Craig and Gráinne de Búrca, *EU Law - Text, Cases, and Materials* (4th ed Oxford University Press, Oxford, 2008), 819.

is of recreational or sporting nature, within this interpretation.[212] Therefore, an activity that is financed via advertising can also be considered as being provided for remuneration, even if the remuneration does not come directly from the user.[213] This interpretation is also in line with the original idea of the EC to protect children on social networks[214] and with the understanding of Article 8 of the GDPR by the Bavarian data protection authority[215].

As a result of the broad interpretation of the term "information society services", the GDPR parental consent requirement will be potentially applicable to a very wide range of online services. The only clear precondition is that personal data is processed by the service and consent is the legal grounds on which this processing is based. Hypothetically, it can be questioned whether any online services offered directly to children can remain outside the parental consent requirement, given the fact that even though there are many websites that can be used without actively providing personal data, such as news or entertainment websites, personal data is often passively collected through tracking techniques (i.e. browser fingerprinting or cookies) and requires users' consent under the e-Privacy Directive[216].
Such a potential over-reliance on parental consent to process children's personal data is hardly desirable, given the deficiencies of consent as a protection mechanism and possible unintended consequences, such as 'consent fatigue' among parents, and potential limitation of children's rights and opportunities (discussed below). Instead of consent, it is worth considering if other lawful grounds such as 'legitimate interests' of data controllers (Article 6.1(f) GDPR) could allow to better safeguard the righs of children and ensure a closer scrutiny when personal data of children is processed, if they are complemented with stricter audits and data compliance mechanisms. In fact, the UK ICO encourages data controllers to rely on the legitimate interest ground, because before invoking it they need to assess the impact of their data processing on children, and consider if such processing is fair and proportionate.[217] In the same vein, due to a high possibility to gain ill-informed consent and the subsequent complications in withdrawing such an invalid consent, some DPAs advise against the use of consent of children or do not recognise consent given by them to legitimise data processing operations.[218]

---

[212] Paul Craig and Gráinne de Búrca, *EU Law - Text, Cases, and Materials* (4th ed Oxford University Press, Oxford, 2008) (provide extensive references to various cases of the Court of Justice relating to the concept of services and remuneration). See for instance: C-70/95 *Sodemare and others/Regione Lombardia (Sodemare)* [1997] ECR I-3395; C-275/92 *H.M. Customs and Excise/Schindler (Schindler)* [1994] ECR I-1039; C-415/93 *Union royale belge des sociétés de football association and others/Bosman and others (Bosman)* [1995] ECR I-4921.

[213] Robert Queck et al., 'The EU Regulatory Framework Applicable to Electronic Communications' in Laurent Garzaniti and Matthew O'Regan (eds), *Telecommunications, Broadcasting and the Internet - EU Competition Law & Regulation* (3rd ed. Sweet & Maxwell, 2010), para. 1-047.

[214] EC confirmed that he main objective of Article 8 is to protect children on social networks. See Council of the European Union, Note from Presidency to Working Party on Information Exchange and Data Protection, 11028/14, 30 June 2014, 87–88.

[215] Bavarian Data Protection Authority, 'Information sheet for the implementation of the GDPR, No. 15', 20 January 2017, <https://www.lda.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf> accessed 3 April 2017.

[216] Article 5(3) of the ePrivacy Directive requires prior informed opt-in consent for storage and access to information on users' terminal equipment.

[217] UK Information Commissioner's Office (UK ICO), 'Consultation GDPR consent guidance', March 2017, <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> accessed 8 April 2017.

[218] Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (OUP, 2007) 211.

If data controllers fully consider all the factors (e.g. the nature and source of the legitimate interest, the aim of the data processing, the impact on children and their reasonable expectations, additional safeguards to limit undue impact on children) and ensure that the interests and fundamental rights of children are duly taken into account[219], the legitimate interest ground can potentially protect children more than the reliance on consent. Even more so, because in case of children the interpretation of the legitimate interest grounds is restricted by the GDPR. Due to the special status of children as data subjects their rights should be considered as overriding the legitimate interest of the data controllers more easily than adult's rights (Article 6.1(f) GDPR).

6.2. Services offered directly to children

The GDPR parental consent requirement concerns online services offered directly to children. Although the intention of the legislator to create a specific protection regime for services that process children's personal data is clear, the exact distinction of services to which the protection applies is a complex issue. In practice, services targeted at children compose only a small part of all services that children can access, use, and sign up to. The latter, so called general and mixed audience services, generate major privacy concerns and anxieties in practice. Various studies in Europe[220] and North America[221] report that from a broad range of websites that children use nowadays, the most popular websites (such as YouTube, Facebook and Google search to name just a few) are often not directed specifically to children (at least not those under 13). Many of such websites claim in their terms of use that their services are not intended for those under 13, even if in practice substantive numbers of young children are in fact active users.[222] As a result, the young "unauthorised users" are treated as adults and presented with the same information and privacy settings, without any consideration of their particular needs, online behaviour or the risks for them in the online environment. Thus, an important question is to what extent the GDPR will reflect reality and to what extent the parental consent requirement will cover general-audience or mixed-audience services and sites?

As the GDPR has just been adopted, the answer to this question is unclear. The Federal Trade Commission (FTC) under COPPA in the US has indicated several criteria to determine whether a website or an online service is directed at children. These criteria include: the subject matter

[219] Article 29 Working Party, 'Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP217', 9 April 2014.

[220] Sonia Livingstone et al., 'Risks and safety on the Internet: The perspective of European children' (LSE, EU Kids Online, London 2011).

[221] Valerie Steeves, 'Young Canadians in a Wired World, Phase III: Life Online.' (MediaSmarts, Ottawa 2014).

[222] Courtney K. Blackwell et al., '*Children and the Internet: Developmental Implications of Web Site Preferences Among 8- to 12-Year-Old Children'*, (2014) 58(1) Journal of Broadcasting & Electronic Media, 1 (data collected from 442 8- to 12-year-old US children to investigate their Internet content preferences indicated that YouTube (26 %) and Facebook (18 %) were the two most favoured websites in this age group). danah boyd et al., 'Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act' (2011) 16(11) *First Monday* (surveyed 1,007 U.S. parents or guardians with children ages 10–14 and found that 19% of 10 years olds, 32% of 11 years olds and 55% of 12 years olds have a Facebook account). Sonia Livingstone et al., 'Risks and safety on the Internet: The perspective of European children' (LSE, EU Kids Online, London 2011) (surveyed 25,142 9- to 16-year-olds in 25 EU countries and showed that 38% of 9- to 12-year-olds have their own profile on social networks).

of the service, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, the age of models, presence of child celebrities or celebrities who appeal to children, language or other characteristics of the website or online service, or whether advertising promoting or appearing on the website or online service is directed to children. [223] Competent and reliable empirical evidence of audience composition and evidence regarding the intended audience are also among the factors to be considered.[224] This "totality of the circumstances test"[225] seems a solid yardstick if applied holistically[226], but might prove problematic if taken in parts. For example, in 2014 the FTC brought a case against TinyCo, deciding that their fantasy apps were subject to the COPPA requirements based mainly on the appearance of these apps'. The FTC claimed that "apps appeal to children by containing brightly-colored, animated characters from little animals or zoo creatures to tiny monsters, and by involving subject matters such as a zoo, tree house, or resort inspired by a fairy tale [and] the language used to describe the apps in the app stores and the gameplay language is simple and would be easy for a child under age 13 to understand".[227] As Hoofnagle noted, "many general-audience apps have childish themes"[228]. This can be well illustrated by the Angry Birds app, which entails child appealing, animated characters, such as stylized colourful wingless birds and green pigs, and thus seems to meet the FTC's criteria for being directed at children, but in fact is widely used by adults in practice.[229]

The FTC has found a solution which, although not entirely uncontested, partially subjects general audience services (i.e. services that are not targeting children but are used by them) to COPPA requirements. It uses the "actual knowledge" test, according to which the COPPA obligations apply to operators of general online services that have actual knowledge that they are collecting, using or disclosing the personal information of children. The general service providers are not obliged to investigate the age of their users actively, but acquiring passive knowledge of children using the service creates obligations under COPPA. Such passive knowledge can be gained, for example, if the operator learns that the person is a child under 13 when dealing with its users, such as responding to an email, seeing the age or the grade in a feedback option, or getting to know the age from a concerned parent, or if a child announces their age in a post seen by an employee of the operator.[230] The actual knowledge standard seems to be problematic in its applicability, as not having actual knowledge of underage service users seems easy to prove, and the standard encourages service provider's ignorance as a means of avoiding compliance. The standard is likely to be met if a child announces their age in a post and the provider monitors the posts, but if the provider does not engage in monitoring, it could

[223] FTC, 'Complying with COPPA: Frequently Asked Questions'<https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Audience>, accessed 1 March 2017.

[224] 16 C.F.R. §312.2. See also FTC, 'Implementing the Children's Online Privacy Protection Act: A Report to Congress' (February 2007) <http://www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf > accessed 3 March 2017.

[225] Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016), 200.

[226] The COPPA Rule's Statement of Basis and Purpose (64 Fed. Reg. 59893) states that the FTC, in making its assessment, should consider "the overall character of the site – and not just the presence or absence of one or more factors."

[227] US v. Tinyco.inc 2014.

[228] Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016), 200

[229] Paul Sawers, 'Nielsen reveals most popular Android apps by age. Angry Birds appeals most to over 35s', 12 December 2011 <https://thenextweb.com/google/2011/12/12/nielsen-reveals-most-popular-android-apps-by-age-angry-birds-appeals-most-to-over-35s/> accessed 5 March 2017.

[230] FTC, 'Complying with COPPA: Frequently Asked Questions'.

be assumed that no one in the organization is aware of the post. The actual knowledge standard has been applied by the FTC in several cases to operators that had age screening in place but allowed children under the age of 13 to register.[231]

The FTC also has a solution for addressing the issue of COPPA applicability to the services that target mixed audiences, such as teenagers under and above 13 or both adults and children. As a general rule, if a service targets children under 13 as one of its audiences (even if not as its primary audience), it is considered to be "directed to children." However, to avoid COPPA applicability to all users in mixed audience services, the amended COPPA Rule foresees a narrow possibility to employ an age screen in order to identify children under 13 and provide COPPA protection only to them. After identifying the users under 13, service providers can choose to either collect parents' online contact information and obtain parental consent or prevent the collection of personal information from these users (e.g. direct them to content that does not collect, use, disclose personal data). Services directed wholly or primarily to children, in contrast to services directed to the users over 13, cannot use the above-mentioned age screen to block children under the age of 13 because of their very nature. According to the FTC, in most cases, a service directed to children must consider all visitors as children without screening them for age and provide to all of them COPPA's protection.

Taking into account the empirical evidence on children's wide use of general-audience services and extensive direct marketing and profiling carried out by these services, it is hard to imagine that the GDPR could not extend the protection to children using these services. The first emerging opinions consider general-audience services, such as Facebook, WhatsApp or Instagram, to fall under the scope of Art. 8 of the GDPR.[232] The next challenging task for the EDPB and national DPAs will be to crystallise the approach on this distinction and to specify related obligations. One of the possible options could be taking a much more protective and rigid approach than the US in COPPA and instead of allowing a simple age screening and blocking users under the established age (in the 13 to 16 age span) in mixed audience services, the GDPR could require appropriate and adequate age verification of users (as discussed below) and protection of those who are under the established age.[233] Such protection would ideally include no or minimal data collection and no disclosure of personal data to third parties – but still provision of interactive and interesting services - or otherwise, if personal data is collected, at least a verifiable parental consent or reliance on other carefully considered legitimate ground, prohibition of profiling and marketing, and age-adapted information.

---

[231] US v. Yelp.inc 2014, US v. Path 2013; US v. Artist Arena 2009, US v. Sony 2008; US v. Xanga.com; Us v.UMG Recordings.inc 2004.

[232] Bavarian Data Protection Authority, 'Information sheet for the implementation of the GDPR, No. 15', 20 January 2017; N. Sonja Kress and Daniel Nagel, 'The GDPR and Its Magic Spells Protecting Little Princes and Princesses. Special regulations for the protection of children within the GDPR' (2017) 18(1) Computer Law Review International 6.

[233] A similar proposal is provided by Karen Mc Cullagh in the context of social networks (SNSs), who claims that "it would have been better to encourage children to provide their true age to SNSs and require SNSs to offer alternative, child-friendly services. This could have been done, for example, by offering platforms to facilitate expression and socialisation by children and permit SNSs to collect performance data from children without parental permission so as to enhance the service offered, but mandate that no profiling and tracking of children's data can be conducted for commercial purposes" (Karen Mc Cullagh, 'The General Data Protection Regulation: a partial success for children on social network sites?', in Tobias Bräutigam and Samuli Miettinen (eds.) *Data Protection, Privacy And European Regulation in the Digital Age* (Unigrafia, Helsinki, 2016) 129-130).

6.3. Consent authorised by the holder of parental responsibility

Article 8 of the GDPR allows consent not only to be given by the holders of parental responsibility over the child but also for the consent to be authorised by them. From the final text of the GDPR, it remains unclear if and under what circumstances parents are allowed to authorise the consent already provided by the child or other individuals on behalf of the child. In this respect, two questions arise: Could the reference to consent authorisation be understood as allowing a joint consent, i.e. a possibility for parents to approve post factum the consent of a child in specific circumstances? Could the circle of holders of parental responsibility include individuals other than parents and legal guardians?

Consent authorisation is not used as a general or child-specific practice under Directive 95/46/EC. It remains to be seen what weight and under what conditions the consent authorisation mechanism will be afforded by the national legislators, the DPAs and the European Data Protection Board in the context of the GDPR. If acknowledged and interpreted broadly, the consent authorisation option can allow the parallel or joint consent of the child and a parent,[234] and thus provide for a more flexible parental consent procedure than is currently explicitly acknowledged in the GDPR. Alternatively, Article 8 will continue to be interpreted as an over protective and fully applicable (except in preventive or counselling services) requirement, that risks limiting children in their online freedoms and opportunities.[235]

The second question relates to the flexibility of the GDPR parental consent requirement to accommodate a wider circle of competent individuals in the definition of the term "holders of parental responsibility". Some national laws affords such flexibility, for example the Irish data protection law allows a grandparent, uncle, aunt, brother or sister of the data subject to consent on their behalf, when the giving of such consent is not prohibited by law.[236] In Malta, the national data protection law not only allows individuals acting in loco parentis but also those acting in a professional capacity in relation to a child to process personal information without necessarily involving parents, if such processing is in the best interest of the child.[237] Similarly, in the US schools may act on the parents' behalf in the educational context when personal data

[234] Article 29 Working Party, 'Opinion 2/2009 on the protection of children's personal data (general guidelines and the special case of schools) WP 160', 11 February 2009.

[235] Milda Macenaite, 'From universal towards child-specific protection of the right to privacy online: dilemmas in the EU General Data Protection Regulation' (2017) New Media and Society (forthcoming) <https://doi.org/10.1177/1461444816686327> accessed 1 April 2017.

[236] Data Protection Act 1988 (updated 14 October 2014), (Article 2A states: "(1) Personal data shall not be processed by a data controller unless […] at least one of the following conditions is met:
(a) the data subject has given his or her consent to the processing or, if the data subject, by reason of his or her physical or mental incapacity or age, is or is likely to be unable to appreciate the nature and effect of such consent, it is given by a parent or guardian or a grandparent, uncle, aunt, brother or sister of the data subject and the giving of such consent is not prohibited by law").

[237] Subsidiary legislation 440.04 Processing of personal data (protection of minors) regulations, 12 March 2004. (the law states: "2.(1) Where any information is derived by any teacher, member of a school administration, or any other person acting in loco parentis or in a professional capacity in relation to a minor, such information may be processed by any of the aforesaid persons if such processing is in the best interest of the minor. (2) Where personal data is being processed as aforesaid, the consent by the parents or other legal guardian of the minor shall not be required if this may be prejudicial to the best interest of the minor. (3) In such a case, no parent or other legal guardian of the minor shall have access to any personal data held in relation to such minor.")

is collected from students for the use and benefit of the school, but not for other commercial purposes.[238] In this case, it can be presumed that the school's authorisation for data collection is based on the parental consent obtained by the school and that a direct parental consent is not required. In order to understand the GDPR in this respect, the interpretation of the "holder of parental responsibility" notion should be aligned with the family law.[239] The concept "parental responsibility" refers to the duties and rights to take care of the child's person (ensure shelter, food and clothes, represent legally, responsibility for the child's upbringing) and look after the child's property. The persons having the parental responsibility of a child are the "holders of parental responsibility", most often being the parents. Nevertheless, if the parents are deceased, not capable or authorised to take care of their child, a guardian such as a relative, a third person or an institution, can be appointed by court to represent the child. Following this definition, the circle of competent persons to provide consent under Article 8 of the GDPR is limited to parents and legal guardians. Thus, if not appointed by the court, it cannot include a wider circle of relatives or expand beyond parents to the professionals working with children. Although inflexible, the choice to limit competent persons to provide parental consent is understandable. Consent in the GDPR is just one of several grounds for data processing and other legal grounds such as compliance with a legal obligation, the performance of a task carried out in the public interest or in the exercise of official authority or legitimate interest of the data controller can also be applicable to the processing of children's personal data by individuals acting in their professional capacity in relation to children, such as teachers in schools. In addition, the parental consent requirement in Article 8 only relates to online services and thus offline data collection from children is subject to general GDPR consent requirements and the relevant national legislation. Parental consent can still be required in relation to offline collection of personal data of children, when this is so required in accordance with national legislation or when children lack the legal capacity to provide valid consent.

6.4. Verifiable and verified consent

The original Commission Proposal required parental consent to be verifiable by stating: "the controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology" (Article 8(1) EC proposal). The final text of the GDPR, however, adopted a different wording and refers to the effort that data controllers should make to verify parental consent. It states that "The controller shall make reasonable efforts to verify (…) that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology" (Article 8(2) GDPR). This change may have different implications for data controllers. While the duty to make reasonable efforts to "verify" consent refers to a one time parental consent verification (i.e. a single verification moment) which

[238] FTC, 'A Guide for Business and Parents and Small Entity Compliance Guide' <https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions> accessed 1 April 2017.

[239] The term "parental responsibility" and all rights and duties of a holder of parental responsibility relating to the person or the property of the child in the EU is defined in Article 1(2) of the Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000 [2003] OJ L 338/1. See also European Commission, 'Practice guide for the application of the Brussels IIa Regulation' <http://ec.europa.eu/justice/civil/files/brussels_ii_practice_guide_en.pdf> accessed 1 March 2017.

should take place prior to the collection of children's personal data, the duty to obtain "verifiable" consent calls for consent to be verifiable at any time (i.e. an ongoing possibility of re-verifying). Even more importantly, the change from "verifiable consent" to "verify consent" means a lower burden on data controllers providing child-directed services online. A reference to "verifiable consent" would have meant that consent could not have been given if it could not be verified and that data controllers should ensure verification through technological means or abstain from relying on consent. The requirement to make reasonable efforts to verify consent is different as it allows the data controller to show that reasonable efforts were made to verify consent and, in circumstances where this was not possible, the data controller may still rely on the unverified consent to process children's data.

The GDPR parental consent requirement is a flexible liability standard. To be compliant, it suffices to make reasonable efforts to obtain verifiable parental consent rather than necessarily obtaining it in all cases. The reference to "reasonable efforts" alludes to the fact that data controllers cannot guarantee verified consent as a final outcome that has to be achieved under the GDPR be that due to a situation beyond their control or due to uncertainty surrounding the technological consent verification capabilities. In the former case, it is not clear how much effort and proof in relation to obtaining consent can be requested from the controllers in situations where it is difficult to acquire verifiable parental consent, for example where discovering the whereabouts or contact information of the parents proves challenging or when the rights of the parents over the child have been terminated and the other legal representative of the child are difficult to reach. How much effort to reach a parent or a legal guardian should be sufficient to demonstrate compliance? How should the exercise of the reasonable efforts be documented and proven? By relying on the reasonable efforts yardstick the burden of proof to demonstrate that a valid consent has been obtained is problematically weakened.[240] In the latter case, data controllers are left with the discretion to choose solutions for obtaining parental consent, taking into account available technology, which might not always be foolproof or lead to very high costs in implementation. If the data controller does not attain parental consent, but still processes the personal data of children, it is important to know how to evaluate if the efforts were reasonable, and establish clear guidelines when less reliable consent verification tools are considered sufficient and how consent verification costs and benefits can be weighted. Otherwise, there is a risk that the vagueness of the reasonable efforts standard can become a shield for the wilful breach or disregard of the parental consent requirement. As the GDPR fails to provide a definition for "reasonable efforts", it is likely that the DPAs and the courts will look into the specific facts and circumstances of the case, examine the controller's efforts and the extent of technological capabilities to obtain verifiable parental consent.

6.5. Consent verification

The GDPR establishes a general requirement to verify parental consent taking into account available technology. Specific parental consent mechanisms that can be used by data controllers to be compliant with the GDPR are not specified and will require further clarification. Lack of clarity on specific methods can lead to GDPR infringements that can

[240] Hornung Gerrit, 'A General Data Protection Regulation for Europe: Light and Shade in the Commission's Draft of 25 January 2012' (2012) 9 *SCRIPTed*, 64.

attract an administrative fine of up to 2% of total global annual turnover or 10 000 000 EUR (Article 83.4).

Similar to the FTC in the US, the EU should specify the possible parental consent methods that are considered to be acceptable in light of available technology to ensure that the person providing consent is the child's parent. The FTC has established a number of acceptable methods for attaining parental consent in order to provide a clear set of choices for industry. It also allows interested parties to submit new verifiable parental consent methods to the FTC for approval. The aim of this provision is to encourage the development of new consent verification methods that are effective but also acceptable for industry and can be used by the applicant or any other party. After the adoption of the amended COPPA rule, the FTC received a number of requests to approve industry proposed verifiable consent methods, thus showing an unprecedented boost in this sector.

In November 2013, the FTC received an application seeking approval of a "social-graph verification" mechanism, a verifiable parental consent method submitted by AssertID, Inc.[241] The proposed method would ask a parent's "friends" on a social network to verify the identity of the parent and the existence of the parent-child relationship. In a letter to AssertID, the FTC noted that the company's proposal failed to provide sufficient evidence that its method would meet the requirements set out under the COPPA rule. Specifically, the FTC considered the approval of this method under the COPPA Rule as premature, noting that there was not yet adequate research or market testing to show the effectiveness of the "social-graph verification" method.[242] Thus such a method cannot ensure that the person providing consent is the child's parent.

In December 2013, based on an application submitted by Imperium, Inc., the FTC approved the use of knowledge-based authentication as a method to verify that the person providing consent for a child to use an online service is in fact the child's parent.[243] Knowledge-based identification is a way to verify the identity of a user by asking a series of challenge questions, typically that rely on so-called "out-of-wallet" information; that is, information that cannot be determined by looking at an individual's wallet and are difficult for someone other than the individual to answer. This authentication method has been used by financial institutions and credit bureaus for a number of years, and has been acknowledged by the FTC and other government agencies as effective for that purpose.

In January 2015, the FTC denied the AgeCheq proposed method, a device-signed parental consent form to obtain verifiable parental consent. It was a multi-step method requiring the entry of a code sent by text message to a mobile device. The FTC decided that the company's proposed mechanism was not compliant with COPPA's requirements regarding the type of parental information that can be collected as a means to verify a parent's identity. The AgeCheq's method did not meet the COPPA requirement of a reasonably calculated age verification method to ensure that the person providing consent is the child's parent or guardian

[241] FTC, 'Letter to AssertID', 12 November 2013 <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-denies-assertids-application-proposed-coppa-verifiable-parental-consent-method/131113assertid.pdf> accessed 1 March 2017.

[242] Ibid.

[243] FTC, 'Letter to Imperium, 23 December 2013', <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-grants-approval-new-coppa-verifiable-parental-consent-method/131223imperiumcoppa-app.pdf> accessed 1 March 2017.

as the person providing consent could easily be the child using the very device on which an app seeking consent was downloaded.[244]

6.6. Verification of age

The GDPR requires that the data controllers obtain verifiable parental consent before processing personal data of children, but there is no particular requirement to authenticate the age of the child, i.e. to verify that the data subject is of a certain age or belong to a certain age group. This is the case despite the fact there have been calls to include the rules on adequate age verification into the GDPR. [245] The initial proposal of the EC provided for delegated acts on this issue, but this proposed provision did not make into the final text of the GDPR.

Age verification may not be necessary for services that by default focus on very young children (i.e. those under 13) which a priori require parental consent from all the users. However, for services targeting teens, mixed audiences or general audience services that are also used by children, in order to fully comply with the GDPR parental consent requirement a service provider needs to know which users are legally competent to consent and from whom parental consent should be sought.

The fact that the GDPR does not refer to age verification is not surprising per se. First, the topic of age verification still raises many sensitive and unresolved questions related to online anonymity, freedom of speech and expression, and privacy vis-à-vis both children and adults online.[246] The idea that all internet users in general audience websites could be asked to provide their age or even worse to identify themselves might not only lead to increased personal data gathering but may also be viewed as disproportionate and thus simply unacceptable. Second, although age verification has been already widely used as a regulatory solution across Europe in online gambling or online sales of age-restricted goods (alcohols, tobacco, etc.), in these

[244] FTC, 'Letter to AgeCheq Inc.', 27 January 2015, <https://www.ftc.gov/system/files/documents/public_statements/621461/150129agecheqltr.pdf> accessed 1 March 2017.

[245] The Article 29 Data Protection Working Party repeatedly stressed the importance of adequate age verification. In the 'Opinion 15/2011 on the definition of consent, WP 187' it advocated age verification use and advised to include into the revised Directive 95/46/EC specific provisions on age verification. As an example it proposed to establish age verification on "sliding scale approach" which would mean that age verification mechanisms depend on the specific circumstances relating to the specific data processing operation, such as the types of personal data that will be processed, the purposes for which they will be processed, eventual risks arising from the processing etc. Equally, Article 29 Data Protection Working Party, in its Opinion 5/2009 on online social networking, WP 163, (12 June 2009, 12) stated: „*The Working Party encourages further research on how to address the difficulties surrounding adequate age verification and proof of informed consent in order to better address these challenges*." The European Data Protection Supervisor also claimed: "If parental consent is necessary, it would be necessary to establish rules on how to authenticate the age of the child, in other words, how to know that the child is a minor and how to verify parental consent." (Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", 22 June 2011.

[246] Berin Michael Szoka and Adam D Thierer, 'COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech' *Progress & Freedom Foundation Progress on Point Paper No. 16.11*, May 21, 2009; Adam D. Thierer, 'Social Networking and Age Verification: Many Hard Questions; No Easy Solutions', Progress & Freedom Foundation Progress on Point Paper No. 14.5, March 2007.

sectors there is extensive evidence related to potential risks and harms associated with the use of such restricted goods and services by minors.[247] It is not the case with privacy and data protection risks and harms, which still lack a detailed and convincing evidence database. The privacy risk and harm assessments debate is still in its embryonic phase[248] and as of yet there is no consensus around what constitutes a privacy harm. Regulators and companies have equally failed to identify a comprehensive list of privacy harms and negative impacts on data subjects.[249,250] Third, some of the existing age verification solutions are not suitable in the data protection context, which requires a granular, more complex approach than verifying that a person is an adult (18 and above). Age verification, as a means of distinguishing between individuals under and over 18, has been used by service providers for controlling access to harmful content, such as offensive or sexually explicit, online content,[251] through the implementation of the Audiovisual Media Service Directive[252]. In practice, unsuitable content is concealed behind a "pay wall" which can be passed by payment methods which are restricted to adults (such as payment by credit card) or age can be established using an independent and reliable database, such as the electoral roll.[253] None of these methods are appropriate for the implementation of the GDPR, as the age thresholds (13 to 16) are various and do not coincide with the legal majority age of 18. This means that there are a limited number of reliable databases on age data for minors, as the majority of the databases (social security number, passport number) only demonstrate that an individual is an adult, without any possibility, at least in their current form, of obtaining granularity in terms of age.[254] Also, the availability of datasets differ from country to country, as for example, in Denmark and Belgium there are more extensive databases on children that could be used. Crosschecking in public databases is reliable and trustworthy, but complex to implement and pose huge privacy concerns because of the sensitivity of the data being processed.

[247] Victoria Nash et al., 'Effective age verification techniques: Lessons to be learnt from the online gambling industry' (Final Report) (2014), Oxford Internet Institute, University of Oxford.

[248] M. Ryan Calo , 'The Boundaries of Privacy Harm' (2011) 86 Ind. L.J. 1131; David Wright and Charles Raab, 'Privacy Principles, risks and harm' (2014) 28(3) International Review of Law, Computers & Technology 277.

[249] National Institute of Standards and Technology, NIST Privacy Engineering Objectives and Risk Model (Discussion Draft) (2014), 3. Some efforts to articulate privacy harms, include: Centre for Information Policy Leadership at Hunton &Williams LLP, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (2014) and 'The Role of Risk Management in Data Protection' (2014).

[250] Victoria Nash et al., 'Effective age verification techniques: Lessons to be learnt from the online gambling industry' (Final Report) (2014), Oxford Internet Institute, University of Oxford, 2.

[251] Recommendation 2006/952/EC of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry [2006] OJ L 378/72, paras. II 1, 2.

[252] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) [2010] OJ L95/1.

[253] The UK regulatory bodies, especially the Authority for Television on Demand (ATVOD), has paved the way within the EU in strengthening the protection of minors in on-demand services and enforcing the "effective Content Access Control System ("CAC System")" "which verifies that the user is aged 18 or over at the point of registration or access" of the service. See ATVOD, 'Rules & Guidance, Statutory Rules and Non-Binding Guidance for Providers of On-Demand Programme Services" (ODPS)', Edition 2.1, Rule 11, 13; ATVOD, 'For Adults Only? Underage Access to Online Porn', 28 March 2014, 7-9.

[254] Victoria Nash et al., 'Effective age verification techniques: Lessons to be learnt from the online gambling industry' (Final Report) (2014), Oxford Internet Institute, University of Oxford.

Finally, despite some efforts in developing standards[255], up until now there are no harmonized procedures to verify a child's age online.[256] Easy-to-use and adequate procedures are unreliable, as determined children can easily circumvent them by lying about their age or pretending to be their parents.[257] The simplest and most widely used, but also the easiest to circumvent, is the self-verification mechanism, where the user is asked for their birth date and access to a service or website is granted if they specify an appropriate age.[258] More advanced age verification methods are based on peer-review, that is, peers decide to grant access to a website or network based on users' profiles and on data collected elsewhere on the web or in the real world. In addition to self-verification, Facebook uses this method. These methods can also be circumvented easily by creating multiple profiles, and in addition, peer-based mechanisms can induce cyber-bulling. A new method of age verification is based on the automatic analysis of the semantics of users' profiles to deduce a user's age rage.[259] These mechanisms are typically difficult to circumvent, but they are complex to implement and not technologically mature, which make them prone to errors in a number of circumstances. Aside from this, it is also only possible to obtain the age range of a user, and not his or her exact age. Reliable alternatives to these methods include offline identity verification, identity verification using eID cards and using biometric data. The offline identity verification is typically implemented by directly contacting the parents or tutors of a minor to verify the age and eventually obtain parental consent to access a website or service. While reliable and effective, the method is also extremely complex. eID cards in contrast, are physical cards with a chip that contains data to perform age and identity verification online. These cards are typically obtained from trustworthy data sources, their use is simple for the user and relatively simple for the service providers to implement, while also being privacy friendly. However, the heterogeneous levels of implementation and the difficulty to enforce it as a standard have limited its popularity. Identity verification methods through biometric data exploit users' unique characteristics, such as fingerprints or iris patterns, to identify them. These mechanisms are reliable and very difficult to circumvent. However, the disclosure of such sensitive personal data raises ethical and privacy concerns. The Article 29 Working Party has called for caution in this respect on several occasions, emphasising that the use of biometrics may have a significant impact on the dignity, privacy and the right to data protection of young children and have potentially harmful effects (e.g. stigmatization or discrimination due to their age or inability to enrol).[260] Moreover, there are additional concrete problems with the use of

[255] The British Standards Institution is facilitating the development of Publicly Available Specification (PAS) 1296 Age Checking code of practice <http://trustelevate.com/age-checking-proof-of-concept-retail-sector/ providers> accessed 1 March 2017.

[256] Article 29 Data Protection Working Party, 'Opinion 15/2011 on the definition of consent WP 187', 28.

[257] Jules Polonetsky, 'Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives', The Future of Privacy Forum, 2009 <https://fpf.org/wp-content/uploads/2009/11/madrid-presentation-online-verification1.pdf> accessed 10 February 2017.

[258] danah boyd et al., 'Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act' 16(11) First Monday, 7 November 2011 (state that "many parents now knowingly allow or assist their children in circumventing age restrictions on general–purpose sites through lying").

[259] Jules Polonetsky, 'Online Age Verification for Our Children, A Report on the Tools and Resources Available for Safeguarding the First Generation of Digital Natives', The Future of Privacy Forum, 2009 <https://fpf.org/wp-content/uploads/2009/11/madrid-presentation-online-verification1.pdf> accessed 10 February 2017

[260] Article 29 Data Protection Working Party, 'Opinion 3/2012 on developments in biometric technologies WP 193', 27 April 2012, 15. Article 29 Data Protection Working Party, 'Opinion 3/2007 on the Proposal for a

biometric data in case of minors. Due to the constantly changing bodily characteristics the biometric data of children become inaccurate and outdated much faster. Therefore, there are practical difficulties (inaccurate data could increase false acceptance or rejection rates and render the whole biometric application unreliable) and legal obstacles as inaccurate data processing contradict to the data quality requirements.[261] Moreover, biometric based methods are still complex to implement and do not allow an exact determination of a user's age.

Given the difficulties associated with finding age verification solutions that would be proportionate and reliable, more guidance and research is needed. The DPAs and the EDPB should take a position on the challenging and largely unresolved issue of age verification and provide guidance on the obligation to employ age verification for specific data collection practices, specific age verification methods and the level of acceptable reliability. As the Article 29 Working Party intends to adopt guidelines on consent in the GDPR in 2017[262], the data protection authorities in UK[263], Ireland[264] and France[265] have started gathering public views on possible solutions for age and consent verification.[266] In this context, UK Information Commissioner's Office (UK ICO) announced that it will start considering the area of children's privacy in order to form its own and European guidance on the issue[267] and issue guidance on how to identify a suitable lawful ground for processing personal data of children, and carry out age verification and parental authorisation.[268]. In Germany, Bavarian data protection authority already issued a commentary on Article 8 and raised critical questions related to its unclear scope and interpretation.[269]

Regulation of the European Parliament and of the Council amending the Common Consular Instructions on visas for diplomatic missions and consular posts in relation to the introduction of biometrics, including provisions on the organisation of the reception and processing of visa applications (COM(2006)269 final) WP134', 1 March 2007, 8.

[261] FIDIS, Biometrics in Identity Managements, <http://www.fidis.net/resources/deliverables/hightechid/int-d37001/doc/19/> accessed 15 February 2017.

[262] European Commission (EC), 'Adoption of 2017 GDPR Action Plan' (Press release), 16 January 2017, <http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083> accessed 15 March 2017.

[263] UK ICO, 'Consultation: GDPR consent guidance', March 2017 <https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf> accessed 10 April 2017.

[264] Data Protection Commissioner, 'Consultation on consent, profiling, personal data breach notifications and certification', March 2017 <https://www.dataprotection.ie/docs/16-03-2017-GDPR-Call-for-consultation-on-consent-profiling-personal-data-breach-notifications-and-certification/1629.htm> accessed 10 April 2017.

[265] Commission Nationale de l'Informatique et des Libertés (CNIL), Consultation publique sur le règlement européen: Consentement, 23 February 2017 <https://www.cnil.fr/fr/consultation-reglement-europeen/consentement> accessed 1 April 2017.

[266] The CNIL public consultation on consent included the following questions: "How can it be determined with certainty that the person concerned is a minor? How can the consent of the holder of parental responsibility be obtained when a minor is under 16 years old? How can specific consent for the collection of sensitive data be gained?".

[267] UK ICO, 'Guidance: what to expect and when' 2016 <https://ico.org.uk/for-organisations/data-protection-reform/guidance-what-to-expect-and-when/>, accessed 13 March 2017.

[268] Sonja Kress and Daniel Nagel, 'The GDPR and Its Magic Spells Protecting Little Princes and Princesses. Special regulations for the protection of children within the GDPR' (2017) 18(1) Computer Law Review International 6, 8.

[269] Bavarian Data Protection Authority, 'Information sheet for the implementation of the GDPR, No. 15', 20 January 2017, <https://www.lda.bayern.de/media/baylda_ds-gvo_15_childs_consent.pdf> accessed 3 April 2017.

7. Moving forward and learning from the US experience

7.1. In the footsteps of COPPA… why is 13 not the best idea?

Although officially the EC has not directly explained or provided any other evidence to justify the choice, little doubt exist that the choice of 13 as the age threshold was influenced by COPPA. To a certain extent the EC itself has recognised the COPPA as being inspiratory. The GDPR's impact assessment published at the same time as the GDPR states: "The specific rules on consent in the online environment for children below 13 years – for which parental authorisation is required – take inspiration for the age limit from the current US Children Online Data Protection Act of 1998"[270]. In addition, the EC admits that following the US legislative choice of the age of 13 would be beneficial for online business. The rules on consent, according to the European Commission's assessment, "are not expected to impose undue and unrealistic burden upon providers of online services and other controllers."[271] In fact, since the adoption of COPPA in 1998, the age limit of 13 has become a de facto standard for parental consent online, used not only by every US-based company, including the most popular social networking sites among children such as Facebook, Snapchat, Instagram, but also copied by a number of European service providers. The EC explicitly confirmed that it views the age of 13 as an existing standard during the debate at the Council of the European Union.[272] Retaining the status quo would not have required so many changes or imposed new burdens on data controllers.

In addition, the US has exerted considerable influence on the GDPR text. Just before the end of the inter-service Consultation, which is one of the last steps in the adoption process of a new Commission legislative proposal, the US started a lobbying campaign against certain GDPR provisions proposed by the EC.[273] In an informal note submitted in December 2011 the US expressed its concerns in relation to diverging standards proposed by the EU GDPR and the obstacles they create vis-à-vis the interoperability between the EU and US privacy regimes.[274] The definition of a child as an individual under 18 in the GDPR was seen by the US as one of such obstacles for commercial interoperability. Defining children "so broadly" according to the US is not advisable or feasible due to practical difficulties and can conflict with older children's rights to freedom of expression and access to information.[275]

---

[270] Commission Staff Working Paper, Impact Assessment, SEC(2012) 72 final. <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf>, 68.

[271] Ibid., 68.

[272] In the Council European Commission "indicated that this [setting the age of consent at 13] was based on an assessment of existing standards, in particular in the US relevant legislation (COPPA)." Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 16 December 2013 <http://register.consilium.europa.eu/doc/srv?l=EN&t=PDF&gc=true&sc=false&f=ST%2017831%202013%20INIT> , 77.

[273] EDRI, 'US lobbying against draft Data Protection Regulation', 22 December 2011 <https://edri.org/us-dpr/> accessed 1 January 2017.

[274] Informal note on Draft EU General Data Protection Regulation, December 2011 <https://edri.org/files/US_lobbying16012012_0000.pdf>; 'Informal Comment on the Draft General Data Protection Regulation and Draft Directive on Data Protection in Law Enforcement Investigations', <https://edri.org/files/12_2011_DPR_USlobby.pdf > accessed 1 March 2017.

[275] Informal note on Draft EU General Data Protection Regulation (n 178) 5.

The decision of the EC to propose the age of 13 as the threshold to allow children to consent to the processing of their personal data, as well as the final choice of the EU legislator to establish the age of 16 as the threshold, but allowing Member States to lower the limit to the age of 13 can be criticised.

First, the age threshold established by COPPA is of questionable use, as the US Congress adopted 13 as a consequence of a political compromise rather than as a well-reasoned or justified choice. Original drafts of this legislation defined children as individuals under the age of 18. When the legislation was introduced it referred to individuals under the age of 16 and only in the final version was the age threshold lowered to 13.[276] This happened eventually to ensure the adoption of the law.[277] Equally proposals to raise the age limit for COPPA coverage were considered in 2010 when the rule was being updated.[278] For example, EPIC recommended Congress to raise the age requirement of COPPA to 18, mainly because "the emergence of social networks and the powerful commercial forces that are seeing to extract personal data on all users of these services, but particularly children, raise new challenges that the original COPPA simply did not contemplate"[279]. The opponents argued that the extension of COPPA to teenagers would diminish privacy and anonymity by requiring age verification and data gathering of a large number of adults and raise profound free speech concerns.[280]

Second, the original intention[281] of COPPA was to protect children's personal information from commercial exploitation, primarily related to aggressive online marketing emerging in 1990s.[282] In fact, as claimed by EPIC, the choice of the age of 13 in COPPA predates many of the most intrusive and complex data collection practises online, such as the extensive behavioural tracking on social networking sites. Therefore, in light of COPPA's legislative history it is strange that none of the EU legislative bodies gathered fresh empirical evidence on the appropriate age threshold for parental consent in the GDPR. Instead of relying on COPPA as a legal transplant, the EU legislator could have questioned - using its own and up-to-date assessment - whether the age limit of 13; 1) can be translated into the completely different Web 2.0 of today and allows for the effective mitigation of risks associated with complex data gathering practises online predated by the original COPPA; 2) reflects the European culture and legal traditions of the EU Member States, as discussed above; and 3) is in line with the

[276] Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016).
[277] EPIC, Testimony of Marc Rotenberg before the Senate Commerce Committee, 28 April 2010 <https://epic.org/privacy/kids/EPIC_COPPA_Testimony_042910.pdf> accessed 4 March 2017.
[278] Ibid.
[279] Ibid., 9
[280] Berin Michael Szoka and Adam D Thierer, 'COPPA 2.0: The New Battle Over Privacy, Age Verification, Online Safety & Free Speech' *Progress & Freedom Foundation Progress on Point Paper No. 16.11*, May 21, 2009; Comments to the FTC from the Center for Democracy & Technology ("Cdt"), The Progress & Freedom Foundation & Electronic Frontier Foundation ("EFF") <https://www.eff.org/files/coppacomments.pdf> accessed 15 February 2017.
[281] There is scholarly debate on the motivation behind COPPA. danah boyd and others argued that COPPA was motivated by privacy (see danah boyd, Urs Gasser and John Palfrey, 'How the COPPA, as Implemented, Is Misinterpreted by the Public: A Research Perspective', Statement to the United States Senate, April 29 2010, <http://cyber.harvard.edu/sites/cyber.harvard.edu/files/COPPA_Hearing_Statement_boyd_Gasser_Palfrey_4-29-10.pdf>; Chris Hoofnagle argues that the motivation related to both privacy and security from online predators (Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016)).
[282] Kathryn C Montgomery and Jeff Chester, 'Data protection for youth in the digital age: Developing a rights - based global framework', (2015)1(4) European Data Protection Law Review 291.

empirical research and evidence on children's Internet use.[283] In addition, the EU legislative bodies should have assessed whether its particular formulation of the parental consent requirement might have a negative impact on the child rights as a whole, which are strongly promoted by the EU itself. Assessments such as this would have allowed adherence to the UN CRC provisions and assessment of the impact of the GDPR by reference to all of the rights within the UN CRC. Ex ante child impact assessment is one of the fundamental steps in the EU child rights mainstreaming model. The lack of empirical evidence and failure to consult with experts and stakeholders, including children,[284] unsurprisingly resulted into a wave of harsh criticism from child rights experts that have accompanied the developments on Article 8 from its conception to adoption.

7.2. Overreliance on (parental) consent and the need to shift protection from parents to data controllers

Although the GDPR establishes parental consent as a medium to protect children online, consent to personal data processing is not a panacea tantamount to giving control to individuals over their personal data in complex networked environments. Consent can provide illusionary control[285] and the agreement to the processing of personal data in situations of imbalance of powers is not delivered freely[286]. A rich body of literature points to the characteristics of networked environments that predetermine power imbalances and limit individuals in asserting control over their personal data.[287] Neither parents nor children can take full responsibility and control of their personal data online, as their choices and data management possibilities are shaped by the design and functionalities of communication spaces.[288] These communication spaces are far from neutral and are created to advance business interests rather than to allow the user to exercise their autonomy and control over their data. Informed consent online is hardly possible due to complex and ubiquitous data collection practises that do not yield to comprehensible privacy policies for service users.[289] In this sense, consent is often a result of a limited understanding of data collection consequences, as users do not actually read long and intricate privacy notices. Privacy policies, for children in particular, are long, complex, difficult

[283] Cf. EU Kids Online project reports <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx>, Global Kids Online research results <http://blogs.lse.ac.uk/gko/results/>. See also Amanda Third et al., 'Children's Rights in the Digital Age: A Download from Children Around the World' (Young and Well Cooperative Research Centre, Melbourne, 2014).

[284] Article 12 of the UN CRC; Committee on the Rights of the Child (CRC) The right of the child to be heard (General comment No. 12) (2009) CRC/C/GC/12.

[285] Laura Brandimarte et al., 'Misplaced Confidences: Privacy and the Control Paradox' (2012) 4(3) Social Psychological and Personality Science 340.

[286] See e.g. Article 29 Data Protection Working Party, 'Opinion 8/2001 on the Processing of Personal Data in the Employment Context WP 48', 13 September 2001.

[287] Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press, 2012). Mireille Hildebrandt, 'Profiling and the Rule of Law' (2008) 1(1) Identity in the Information Society 55.

[288] Alice E Marwick and danah boyd, 'Networked privacy: How teenagers negotiate context in social media' (2014) 16 New Media & Society 1051.

[289] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (May 25, 2016) <https://ssrn.com/abstract=2784123> accessed 1 March 2017.

to find[290] and easily confusing in their discourse (valorising 'sharing' and 'control', despite the extensive collection of children's data).[291] Consent can hardly be considered freely given when refusal to consent leads to social exclusion[292] given that important online services have no real alternatives. Various scholars have emphasised the weaknesses of consent as a protection mechanism online.[293] Many others have demonstrated that strengthening consent will not lead to a greater individual control for individuals over personal data[294] and that consent cannot always be considered a legitimate ground for data processing.[295]

Yet, the GDPR is based on the premise that children can be protected through informed parental consent. As noted by Savirimuthu, 'since notice and consent are effectively meaningless, children are left with the predicament of making complex and undesirable trade-offs, resorting to social stenography techniques or accepting that the costs of obscurity is exclusion from participation in communities'.[296]

Not only consent in general but also parental consent in particular suffers from significant limitations both in terms of adequate protection and impact on children's rights. As regards adequate protection, there are many potential reasons why parental consent does not necessarily mean an increased protection of personal data for children. The GDPR requires consent to be sought from parents for all types of information society services in different sectors. An

[290] Jacquelyn Burkell, Valerie Steeves and Anca Micheti, 'Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand' (report), March 2007 <http://www.idtrail.org/content/view/684/42/> accessed 10 April 2017; Sara M Grimes, 'Persistent and emerging questions about the use of end-user licence agreements in children's online games and virtual worlds' (2013) 46(3) *UBC Law Review* 681.

[291] Valerie Steeves, 'Terra Cognita: Surveillance of Young Peoples' Favourite Websites' in Emmeline Taylor Tonya Rooney (eds) *Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People* (Routledge, 2017).

[292] Ruth Furlong and Facer Keri, Beyond the Myth of the 'Cyberkid': Young People at the Margins of the Information Revolution (2001) 4(4) Journal of Youth Studies 451.

[293] Alessandro Mantelero, 'The future of consumer data protection in the E.U. Rethinking the "notice and consent" paradigm in the new era of predictive analytics' (2014) 30 Computer Law & Security Report, 643. Bart W. Schermer, Bart Custers and Simone Van der Hof S, 'The crisis of consent: how stronger legal protection may lead to weaker consent in data protection' (2014) 16(2) Ethics and Information Technology 171; Eleni Kosta, *Consent in European data protection law* (Brill/Martinus Nijhoff Publishers, 2013), 395-396.

[294] Lokke Moerel and Corien Prins, 'Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things' (May 25, 2016) <https://ssrn.com/abstract=2784123> accessed 1 March 2017; Bert-Jaap Koops, The trouble with European data protection law (2014) *4(4) International Data Privacy Law 250.* Brendan Van Alsenoy, Eleni Kosta and Jos Dumortier, Privacy notices versus informational self-determination: Minding the gap (2014) 28(2) International Review or Law, Computers & Technology 185.

[295] Jean-Marc Dinant and Yves Poullet, The internet and private life in Europe: Risks and aspirations in A T Kenyon and M Richardson (eds), *New Dimensions in Privacy Law: International and Comparative Perspectives* (CUP, 2006), 72. ("Nevertheless consent does not appear to us to be a sufficient basis for legitimacy. We think that, in certain cases, the legitimacy of processing that is even backed by a person's specific, informed and freely given consent may be called into question. There are three reasons that support this view. First, consent that has even been obtained by fair means cannot legitimise certain processing that are contrary to human dignity or to other key values that an individual cannot relinquish. Second, consumers must be protected against practices that involve their consent being solicited in exchange for economic advantages. Finally, the question of the protection of privacy is not just a private matter but brings social considerations into play and calls for the possibility of intervention and marginal supervision by the authorities.")

[296] Joseph Savirimuthu, 'Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests?' in I Iusmen and H Stalford H (eds) *The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions* (Columbia University Press, 2016), 234.

overload of consent requests may result in 'consent fatigue' among parents, when a constant consenting process becomes a disturbing irritation rather than a serious choice and can make the entire parental consent provision illusionary. The effectiveness of parental consent verification is still questionable, as due to the ambivalent and soft wording of the Article 8 in the GDPR, age verification depends on available technology and efforts of the industry that are considered 'reasonable'.[297]

In addition, the restriction of access to online services through parental consent, as formulated in the GDPR, might also have a negative impact on children's rights and autonomy.

Given that the consent requirement in the GDPR is fully applicable to all children under the nationally chosen age or the default age of 16 for all data processing cases that take place on the basis of consent, except for the preventive or counselling services, children might be restricted in their right to freedom of expression on the Internet. The UN CRC affirms that children are entitled to freedom of expression "which includes the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice". The consent requirement in the GDPR positions parents as arbiters in deciding what is both allowed and beneficial for their children, without formally allowing children to influence their decisions. As noted by the Belgian Privacy Protection Commission, "parental consent should not be a mechanism permitting a parent to override the child's decision unless there is a serious risk that the child will not correctly appreciate the consequences of its decision or that its natural naivety will be exploited."[298] Parents may not always be in a position to fully grasp the best interest of the child. There could be cases of disagreement between parents and children over the usefulness and risks in relation to social media, and emotional, moral-panic driven or simply unjustified consent request rejections from parents. Counterintuitively, parents may become potential invaders of their children's privacy. For example, by using the right of access to personal data on behalf of their children, parents could monitor their children's online activities[299]. Also, parental consent mechanisms may become parental control systems and restrict the online freedoms of children[300]. Finally, the GDPR does not sufficiently take into account the right of the child to be heard, a fundamental principle of the UN CRC, and guarantee that the right of the child to express their views freely in all matters affecting them is taken into account in accordance with the age and maturity of the child.

Given the weaknesses of consent in general and parental consent in particular, the GDPR places an excessive burden on parents and children to make informed decisions about their personal data processing in the complex technology and data-driven environment.

More realistic possibilities to affect digital data collection practises and respond to children's needs and expectations would seem to entail shifting the responsibility from parents to data

[297] It could be claimed that in certain cases consent verification might become obligatory under Article 35 of the GDPR when data controllers perform data protection impact assessments and determine the appropriate measures (e.g. consent verification mechanisms) to comply with the GDPR.

[298] Opinion (Avis) no. 38/2002 on the protection of the privacy of minors on the internet <http://www.privacy.fgov.be> accessed 1 March 2017.

[299] Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016).

[300] Simone van der Hof, 'No child's play - Online data protection for children' in Simone van der Hof, Bibi van den Berg and Bart Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Information technology and law series (24) (Springer with T. M. C. Asser Press, The Hague, 2014).

controllers. Instead of asking parents to control children's data collection through consent, the law could forbid some undesirable data collection practises through restrictions on the activities of data controllers. This would be in line with the thinking developed in the US after almost two decades of the COPPA experience. Hoofnagle claims that the real value of COPPA is in its limitation on personal data collection, use and retention through obligations on data controllers instead of the focus on parental consent requirement.[301] Montgomery echoes this view and argues that some children's data collection practises, such as profiling, behavioural advertising, cross-platform tracking, geolocation targeting should not be allowed by COPPA even with parental permission.[302] Similarly, Thierer claims that aside from education and empowerment, targeted enforcement of unfair and deceptive practices should be a way forward rather than parental consent and age verification expansion.[303] Boyd et al. suggest "that policy–makers shift away from privacy regulation models that are based on age or other demographic categories and, instead, develop universal privacy protections for online users" and "provide parents with recommendations about the appropriateness of various sites for children of different ages and the various risks that users may face".[304]

The GDPR entails provisions that limit the processing of children's personal data. The use of the legitimate interest of the data controller as a ground for lawful children's data processing is restricted in the GDPR. When the data subject is a child, it is highly probable that the legitimate interest of the controller are overridden by the interests or rights and freedoms of the child. Nevertheless, the legitimate interest ground can still be used by the data controllers in relation to children's data, but the assessment should be documented and the interest balancing exercise in general is likely to favour children as data subjects.

Recital 38 of the GDPR generally emphasises that specific protection should be afforded to children against marketing or profiling. Recital 71 refers to automated decision making based on profiling and states that such a measure should not concern children. This alludes to the conclusion that the profiling of children is prohibited, but upon closer scrutiny of both above-mentioned recitals, it appears that only automated decisions leading to legal effect or otherwise significant effects on children taken based on profiling are entirely forbidden. Taking into account the overarching objective of the GDPR to provide children as data subjects enhanced protection and the specific intention of the Member States to protect children against profiling clearly seen in the Council debate (discussed above), it would have been desirable to explicitly exclude children from profiling. It has been widely acknowledged that behavioural advertising is "outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing'[305]. As illustrated by Mc Cullagh "children (and indeed most adults) are unlikely to be aware that inferences can be made from their disclosures—for instance, that "liking" curly fries on Facebook is indicative of high intelligence or that "likes" can be used to predict race

[301] Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016), 215. ("(t)he real privacy protection in COPPA comes from its non-consent-related provisions, such as limits on data collection, use and retention")

[302] Kathryn C Montgomery and Jeff Chester, 'Data protection for youth in the digital age: Developing a rights - based global framework', (2015)1(4) European Data Protection Law Review 291.

[303] Adam D Thierer, 'Kids, Privacy, Free Speech & the Internet: Finding the Right Balance' (August 12, 2011). <http://ssrn.com/abstract=1909261> accessed 13 February 2017.

[304] danah boyd et al., 'Why parents help their children lie to Facebook about age: Unintended consequences of the 'Children's Online Privacy Protection Act' (2011) 16(11) *First Monday*.

[305] Article 29 Data Protection Working Party, 'Opinion 02/2013 on apps on smart devices WP 202', 27 February 2013.

or sexual orientation with a high degree of accuracy—and that both disclosed and inferred information can be used to generate profiles and produce targeted adverts".[306]

Yet, the vagueness related to children and profiling imbedded in the GDPR can be explained by practical challenges. It is questionable how effectively an explicit prohibition to profile children could have been enforceable in practice. It is still difficult to reliably distinguish between adults and children online.[307] An obligation to identify children in order to completely remove them from all targeting may lead to excessive data collection of a large number of adults, and instead of protecting one's privacy and anonymity online, could diminish and erode both.

The above mentioned restrictions, if effectively implemented, could have provided an alternative to the parental consent requirement as a protection model. Such restrictions on the collection of children's data, coupled with the respect for the fair data processing and accountability principles, would be better suited to diminishing its commercial exploitation in complex marketing, tracking and targeting systems, than parental consent.

7.4. Deciding on the (single) age threshold

The GDPR sets a single age limit of 16 after which all children can be deemed competent to consent to the processing of their personal data, unless a Member State's national laws set a lower age which cannot go below the age of 13. A number of problems and challenges can be identified that need to be addressed before the GDPR comes into force.

Given the many different sectors and data collection practises, the choice of fixing a single age limit for consent in all data processing activities online has serious flaws. In order to guarantee adequate protection for children as data subjects but not excessively limit their online behaviour and rights, the context and data collection purpose should be taken into account. Different information society services might carry significantly different risks to a child's online safety and privacy. One and the same child may need protection for one data processing purpose, and may be able to autonomously consent to another. This is well illustrated by the case law in Germany. The Higher Administrative Court of Lüneburg[308] in a case related to video surveillance considered that the consent of a child may in general be invalid, if the child had not yet reached at least the age of 14 years. However, in 2012, the Higher Regional Court of Hamm[309] decided that it cannot be presumed that children between the age of 15 and 18 years would always have the required capability to foresee the consequences of the respective data processing operations. This case related to the processing of personal data for a sweepstake. The imposition of a single legal age-limit may disproportionally restrict the rights and opportunities for the child, irrespective of a child's own levels of competence in a specific

[306] Karen Mc Cullagh, 'The General Data Protection Regulation: a partial success for children on social network sites?', in Tobias Bräutigam and Samuli Miettinen (eds.) *Data Protection, Privacy And European Regulation in the Digital Age* (Unigrafia, Helsinki, 2016).
[307] Simone van der Hof, 'No child's play - Online data protection for children' in Simone van der Hof, Bibi van den Berg and Bart Schermer (eds), *Minding Minors Wandering the Web: Regulating Online Child Safety*. Information technology and law series (24) (Springer with T. M. C. Asser Press, The Hague, 2014).
[308] Germany, Case No. 11 LC 114/13.
[309] Germany, Case No. I-4 U 85/12.

context. Therefore, it might be worth considering the adoption of different age limits for different data collection areas and practices in the 13 to 16 age span. This might prove to be complex for children and parents to understand, but could provide more flexibility and account for the complexity and potential negative impact on children caused by specific data collection practices.

There could be several ways of determining the specific consent age limits and respective data collection areas. The Member States could adopt their national laws as they have the possibility to depart from the Regulation default age of 16. Detailed age limits and the identification of more and less risky data collection areas or purposes is unlikely to be achievable in the national data protection framework or other specific laws. In addition, for the industry this would result in increased disparity and an even more patch worked picture in every national jurisdiction. Codes of conduct at the European level therefore would seem to be a more flexible and less burdensome way of creating standards that account for children's vulnerabilities in a specific activity or sector, instead of treating all children as a homogeneous group of data subjects. As mentioned below, the GDPR creates conditions for the adoption of more effective codes of conduct.

If the Member States chose to legislate and lower the age threshold to 13, the industry codes of conduct could still go beyond this age requirement and guarantee stringent protection in specific data collection scenarios. Increasing the age limit up to 16 in voluntary codes of conduct in specific areas is therefore an option which would be in line with the GDPR requirements and provide added value by offering more protection for children's personal data in specific sectors.

During the GDPR adoption process the European institutions provided no evidence based on which the proposed age threshold would be grounded. The choice of the most appropriate age limit between 13 and 16, be it in national law or in self-regulatory initiatives, should be based on extensive empirical research. Social and behavioural sciences should be the first areas in which legislators gather solid and profound scientific evidence to justify any given age limit.

Also, until now, no public consultation to incorporate the voice of children has taken place.[310] During the GDPR adoption process adult driven discourse marked by a very protectionist stance in relation to children as internet users dominated. However, highly paternalistic and restrictive views have problematic consequences for children as rights holders, as 'such a narrow lens positions children solely as vulnerable victims, neglecting their agency and rights to access, information, privacy and participation'.[311] Consultations with relevant stakeholders, not only governments, industry, civil society, educational actors, but also children and parents themselves, should take place before taking decisions that affect children's rights and interests. It is well established that the views of children themselves should be considered in policymaking and the preparation of national laws related to the use of children's personal data, as well as in their evaluation.[312] As noted by the Committee on the Rights of the Child,

[310] Joseph Savirimuthu, 'Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests?' in I Iusmen and H Stalford H (eds) *The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions* (Columbia University Press, 2016).

[311] Sonia Livingstone, John Carr and Jasmina Byrne, 'One in Three: Internet Governance and Children's Rights' (2015) Global Commission on Internet Governance Paper Series No. 22.

[312] Committee on the Rights of the Child, The right of the child to be heard (General Comment No. 12) (2009) CRC/C/GC/12.

'including children should not only be a momentary act, but the starting point for an intense exchange between children and adults on the development of policies, programmes and measures in all relevant contexts of children's lives'.[313]

7.7. Pursuing the idea of age verification through innovative technological solutions

The implementation of Article 8 of the GDPR provides an opportunity for the EU to explore the different challenges and opportunities in adopting innovative online methods of age verification. Lessons can be learnt from national efforts and failures in the EU Member States and in the US. In the EU, several national age verification schemes using personal ID numbers have been facing shortcomings in terms of adequate enforcement, disproportionate data collection, and usability. In Germany, an attempt to use an age verification system based on the identity card or passport number coupled with the postal code of the city of its issuance has been declared by the German Federal Supreme Court as an effective barrier to prevent minors from accessing online age-restricted content.[314] In Belgium, the kids-ID card has been used as an online identification and age verification tool.[315] Using an integrated PIN and a card reader, from the age of six, children can identify themselves on the Internet with their kids-ID card and access online child-friendly chat rooms. However, this age verification tool has been criticised as too intrusive and disproportionate due to the use of the National Registry identification number embedded in the eID card revealing the date of birth and the gender of the child when only the identification of an individual as a child would be sufficient.[316] Also, the system was abolished quickly due to the fact that no children were found in the child-friendly chat rooms.[317] A more successful effort has been the SaferChat application implemented by the STORK project.[318] With the aim to implement EU-wide interoperability of electronic identities, the SaferChat created a safe online platform allowing for children from different EU Member States to communicate in chat rooms, using their national eIDs for identification, authentication and authorisation. Yet, the SaferChat application has been tested only as a pilot and did not yet lead to its sustainability in the long term or a wider take-up throughout the EU. In the US, as mentioned above, COPPA relies on users' self-assertion of their age which, as a method, is as easy to use as it is to circumvent. Children may often not be genuine in registering, use personal data that may not belong to them, and circumvent the age gating systems, for example by deleting cookies and restating a higher age. Lack of age verification if one of the main reasons for which COPPA has been widely claimed to be ineffective[319] and faces significant implementation and enforcement challenges. Notwithstanding this fact, the EC almost literally

[313] Ibid., 5.
[314] See BGH vom 18.9.2007 – I ZR 102/05 – ueber18.de – OLG Düsseldorf, Zeitschrift für Urheber- und Medienrecht 2008, pp. 511-516
[315] The Belgian E-Id card has been designed to provide various functions: standard functions such as the proof of identity, a travelling document and a card for protection in emergency situations, in addition to acting as the online identification and age verification tool.
[316] Eva Lievens, 'Protecting children in the new media environment: Rising to the regulatory challenge?' (2007) 24(4) Telematics and Informatics 315.
[317] Eva Lievens, *Protecting Children in the Digital Era* (Brill, 2010) 249, 408.
[318] STORK project, Pilot 2, Safer Chat - To promote safe use of the Internet by children and young people <https://www.eid-stork.eu/pilots/pilot2.htm> accessed 1 March 2017.
[319] Chris J Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (CUP, 2016).

copied the COPPA parental consent requirement[320] in its proposal for the GDPR, ignoring the critics related to its ineffectiveness, without considering any alternatives of a more nuanced approach.

The EU should not blindly follow the US COPPA example, but pave the way in developing and adopting innovative and more effective age verification mechanisms. Given the challenges, there is a need to look for innovative age-verification mechanisms that are: 1) privacy-enhancing and respect data minimisation; 2) user-friendly and do not overburden the service providers; 3) do not limit children's opportunities provided by the Internet. The search for such solutions can be aligned with the EU's renewed interest and advancements in online authentication, attribute-based ecosystems and public e-ID schemes. The new Regulation 910/2014 on electronic identification (eIDAS Regulation) enables the adoption of secure eID throughout the EU and, accordingly, can facilitate age-related eligibility checks. In the context of the Audio Visual Media Services Directive, the European Commission asked content platform providers to explore the possibilities of leveraging secure eID, to conduct age-checks, in order to restrict children's access to harmful online content.[321] Consequently a multi-stakeholder group entitled the Alliance for Child Protection has been formed to examine how companies can use secure eID to improve the e-safety of children and develop codes of conduct.[322]

As age verification can range from verifying that an individual is above a certain age threshold, to knowing the exact age of a person and identifying an individual based on his age and other pieces of personal data (name, ID number, etc.), these various solutions have diverse implications to internet users' privacy. The EU should favour the least intrusive age verification method, such as relying on anonymous credentials and attributes through the creation of an appropriate legal framework, policies, technical architecture and standards. The use of attribute-based credentials in implementing Article 8 of the GDPR looks particularly promising, due to the advantages of minimal data disclosures and unlinkability.[323] In attribute-based schemes rather than verifying the full identity of an internet user, only a particular attribute, such as age, could be cross-checked in order to establish an internet user's eligibility to access an online service. Private technical architectures and standards are emerging on the market that are based on attributes and partial identity disclosure to prevent ineligible users from buying age-restricted goods, accessing age-restricted content (e.g. adult content, specific categories of advertising) or using age-restricted online services (e.g. dating agencies).[324] These

[320] Compare, for example, COPPA: "An operator must make reasonable efforts to obtain verifiable parental consent, taking into consideration available technology" with the EC Draft proposal: "The controller shall make reasonable efforts to obtain verifiable consent, taking into consideration available technology".

[321] European Commission, Commission updates EU audiovisual rules and presents targeted approach to online platforms (Press release), Brussels, 25 May 2016 <http://europa.eu/rapid/press-release_IP-16-1873_en.htm>.

[322] European Commission, 'Commission to broker a new Alliance to better protect minors online', 25 May 2016 <https://ec.europa.eu/digital-single-market/en/news/commission-broker-new-alliance-better-protect-minors-online> accessed 5 March 2017.

[323] On attribute-based credentials see Kai Rannenberg, Jan Camenisch and Ahmad Sabouri (eds), Attribute-based Credentials for Trust: Identity in the Information Society (Springer, 2015).

[324] See e.g. Trust Elevate's Age Check solution based on the attribute exchange ecosystem for pseudonymous age-related eligibility checks online and the development of Publicly Available Specification (PAS) 1296 Age Checking code of practice <http://trustelevate.com/age-checking-proof-of-concept-retail-sector/> accessed 5 March 2017.

solutions that aim for pseudonymous and reliable age checks online could be considered when implementing Article 8 of the GDPR.

There is hardly a 'one-size fits all' solution for age verification that reflects the needs of different online service providers.[325] Different information society services with their particular data collection practises pose different degrees of risks to children as data subjects. As a result, methods of age verification that afford lower level of assurance might be adequate in lower risk online services, leaving high assurance options for high risk information society services.[326] This sliding scale approach is in line with the risk-based approach embodied into the GDPR, implying that the obligations of data controllers can be scalable according to the level of risk that their data processing poses to the rights and freedoms of the data subjects. The GDPR allows for the implementation of the sliding scale approach through data protection impact assessment and the adoption of safeguards, security measures and mechanisms to mitigate the risks, such as age verification of varying levels of assurance. High levels of assurance could be required for data processing involving profiling, marketing and other practises from which the GDPR considers that children merit specific enhanced protection.

Sliding scale age verification would less likely result in limiting online opportunities and benefits for children online, as the costs of obtaining age verification might lead to higher costs and lower revenues for data controllers, and consequently less valuable and interesting content for children. Proportionality is important for service providers, in the sense that "the costs of age verification measures to be introduced must deliver enough benefit to the customer and the company to counter any additional costs (not just financial, but also in terms of time, convenience etc) imposed".[327]

7.8. Consent verification driven by data controllers

When determining acceptable parental consent verification methods, the EU could learn some lessons from COPPA. In essence, the US embraces the co-regulation model, according to which if industry has a problem, the industry has the burden of solving it, and therefore it can propose responsible solutions approved by a regulator.[328] The FTC has a long history in working with the industry on methods of obtaining verifiable parental consent and deciding what methods are "reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent". The EU could equally establish a number of acceptable methods for gaining parental consent, at the same time encouraging interested parties to submit new verifiable parental consent methods for approval. It would actively incentivise the development of new age verification methods that are not only effective but also acceptable by the industry and suitable for specific sectors.

---

[325] Victoria Nash et al., 'Effective age verification techniques: Lessons to be learnt from the online gambling industry' (Final Report) (2014), Oxford Internet Institute, University of Oxford.

[326] Ibid., 3 (they claim "the level of assurance (reliability) needed will vary across transactions: customer registration for an online gambling account will require both a wider range of information, and a higher level of assurance than would be needed to process the sale of a 15-rated DVD, for example.")

[327] Victoria Nash et al., 'Effective age verification techniques: Lessons to be learnt from the online gambling industry' (Final Report) (2014), Oxford Internet Institute, University of Oxford.

[328] Ira Rubinstein, 'Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes' (2011) 6 A Journal of Law and Policy for the Information Society 356.

Codes of conduct could be one possible way to create standards for effective consent verification and specify Article 8 of the GDPR. Both the current DPD and the future GDPR encourages data controllers to adopt codes of conduct of industry associations that take account of the specific features of the various processing sectors. Codes of conduct are considered as "market driven tools for application" of the GDPR provisions[329] and are attractive due the socio-technological expertise of the industry, innovation, reactive speed and reduced costs for the public bodies.[330] The GDPR provides additional incentives for data controllers to create or adhere to approved codes of conduct: adherence to a code of conduct may demonstrate compliance with the obligations of data controllers, provide the basis for international data transfers, be a positive factor in a Data Protection Impact Assessment and when fines are being imposed upon the adherent party. The GDPR explicitly refers to the protection of children and the manner in which parental consent should be obtained as one of the possible areas in which the GDPR's requirements could be specified (Article 40 GDPR). Thus, parental consent verification methods could be proposed by the industry through the codes of conduct.

Nevertheless, in order to ensure that self-regulation is accountable, efficient and able to deliver on its societal goals[331], the EU should actively participate in the formulation of self-regulatory rules, and their effective monitoring and enforcement. Under the Directive 95/46/EC, the success of voluntary data protection codes has been very limited. The number of codes approved by the national data protection authorities vary significantly from one Member State to another. At the European level, very few organisations representing specific sectors have tried, and only one of them has managed to draw up a code that was fully endorsed by the European data protection authorities.[332] The process of self-regulation took several years and was not necessarily shorter than a legislative procedure. Also, self-regulatory codes were limited in their ability to protect children as internet users, because of vague language, inadequate enforcement and monitoring mechanisms, and low market penetration.[333] In the area of online child safety, although little research is available on the actual impact of self-regulatory systems, the questionable efficacy of the major existing voluntary initiatives, such as the Safer Social Networking Principles for the EU, raise doubts as to their full implementation and compliance.[334] Stronger EU participation in the self-regulatory process, in particular rule formulation and enforcement, could help to achieve a better balance between the interests of children to exercise control over their personal data and the desire of businesses to valorise and profit from users' personal data. The GDPR, in contrast to the DPD, takes a step in that direction and requires: a) data protection authorities to evaluate whether the code

[329] Irina Vasiliu, 'Speech at the 7th Plenary Meeting of the Community of Practice for Better Self- and Co-Regulation. Synthesis of the Plenary', 24 June 2016 <http://ec.europa.eu/information_society/newsroom/image/document/2016-28/cop_7_-_synthesis_of_the_discussions_16585.pdf>

[330] Eva Lievens, 'Protecting Children in the New Media Environment: Rising to the Regulatory Challenge?' (2007) 24(4) Telematics and Informatics 315.

[331] European Commission, Principles for Better Self- and Co-Regulation <https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/CoP%20-%20Principles%20for%20better%20self-%20and%20co-regulation.pdf> accessed 2 February 2017.

[332] The only finalised code of conduct on the EU level is the 'European Codes of practice for the use of personal data in direct marketing' including an annex on online direct marketing by FEDMA <http://www.fedma.org/index.php?id=56> accessed 15 January 2017.

[333] Milda Macenaite, 'Protecting Children's Privacy Online: A Critical Look to Four European Self-regulatory Initiatives' (2016) 2 European Journal of Law and Technology.

[334] Jos De Haan et al., 'Self-regulation' in Brian O'Neill, Elisabeth Staksrud and Sharon McLaughlin (eds) *Towards a better Internet for Children. Policy pillars, player and paradoxes* (Nordicom, 2013).

complies with the GDPR and, approve it, as well as register and publish the code; b) an independent body, which has an appropriate level of expertise and is accredited by the competent supervisory authority, to monitor compliance with codes of conduct.

8. Conclusions

The growing importance of children's rights in EU policy making, empirical evidence vis-à-vis the risks for children and excessive and complex children's data collection practices online have driven the recognition in Europe that children's personal data deserves specific protection. The EU General Data Protection Regulation, which will be applicable from the 25th of May 2018, has established the requirement to obtain parental consent for the processing of the personal data of a child below the age of 16 years (unless national laws specifies a lower age threshold which cannot be lower than 13) when offering information society services (Article 8). Under the current Directive 95/46/EC, which has no specific rules on the consent of minors, the requirements related to the age and validity of consent have been diverging within the EU. Member States took three distinct approaches to regulate children's capacity to provide consent to their data processing, namely an objective bright-line, "regulation by analogy", and a subjective capacity-based approach.

The analysis of the legislative history of Article 8 in the GDPR reveals the lack of well-reasoned justifications and evidence in terms of the substantive requirements adopted in the final version. With most of the GDPR debate being focused around articles with a direct economic impact on data controllers' activities and the Digital Single Market rather than the protection of vulnerable data subjects, Article 8 witnessed only sporadic renewals of interest during the debates in the EU institutions.
The European Commission almost literally copied the parental consent requirement from COPPA in its proposal for the GDPR, without taking into account the criticisms related to ineffective parental consent and age verification mechanisms or considering any alternatives of a more nuanced approach to child protection. Despite many valuable amendments being registered, the discussions at the European Parliament did not lead to major substantive changes either. The Council has only substantially deviated from the original GDPR proposal on the age of consent. It initially increased the age limit of consent to 16 years and in the last minute of negotiations took a flexible approach leaving the decision partially to the Member states. As a consequence, this left the EU without coherent and uniform age threshold in the European Digital Market and undermined the much-anticipated harmonisation effect of the GDPR. In summary, none of the EU institutions failed to employ an up-to-date means of assessment, question the age limit for consent, assess the impact on children's rights and the effectiveness of a particular formulation of the parental consent requirement, and to consider adopting a more nuanced version of parental consent.

Due to the failure to use well-reasoned justifications and evidence during the legislative process and the ongoing lack of guidelines, the GDPR parental consent requirement faces many practical challenges related to its interpretation and implementation. First, the requirement is applicable to information society services offered directly to a child. As information society services are normally provided for remuneration, this causes uncertainty as to the particular material scope of Article 8, especially its applicability to free services. Second, the requirement concerns online services offered directly to children, but it is complicated to draw the exact

distinction between services to which the protection should apply. The extent to which the GDPR parental consent requirement will cover general-audience or mixed-audience services and sites remains unclear. The FTC solution of subjecting different services to a parental consent requirement through the "totality of the circumstances test" and "actual knowledge test" is useful, despite its flaws. Third, as the GDPR allows consent authorisation by the parents or the holders of parental responsibility over the child, it remains unclear if the reference to consent authorisation can be understood as allowing a joint consent and if the circle of holders of parental responsibility can include individuals other than parents and legal guardians. Fourth, to comply with the GDPR it suffices to make reasonable efforts to obtain verifiable parental consent rather than guarantee verified consent as a final outcome. It is not clear how much effort and proof in relation to obtaining consent can be requested from the controllers in order to sufficiently demonstrate compliance nor how reasonable efforts should be documented and proved. Fifth, specific parental consent mechanisms that can be used by data controllers to be compliant with the GDPR require further clarification and the guidance of the FTC on COPPA can be informative in specifying adequate and GDPR-compliant consent verification methods. Finally, the GDPR does not explicitly require the verification of a child's age, and thus more specification is needed on the relationship between consent and age verification, and the need for concrete proportionate and reliable age verification solutions.

Drawing on COPPA in the US, we identified pitfalls to be avoided and lessons to be learned when moving forward in the implementation of the EU parental consent requirement. Given the weaknesses of consent in general and parental consent in particular, the GDPR places an excessive burden on parents and children to make informed decisions about their personal data processing in the complex technology and data-driven environment. Instead of asking parents to control children's data collection through consent, restrictions on the most undesirable data processing practises in relation to children should be enforced. Effective GDPR restrictions on children's data collection such as prohibition of profiling, marketing, the use of legitimate interest as a ground to process children's data, may provide an alternative to the parental consent requirement as a protection model. Purpose dependent restrictions on the collection of children's data would be better suited to diminishing its commercial exploitation in complex marketing, tracking and targeting systems, than parental consent.

The implementation of Article 8 of the GDPR provides an opportunity for the EU to address the different challenges and opportunities in adopting innovative online methods of age verification. Instead, of purely relying on the internet users' self-assertion of their age, as provided in the COPPA regime in the US, the EU should explore innovative, effective and privacy-friendly age verification mechanisms, aligning them with the advancements in online authentication, attribute-based ecosystems and public e-ID schemes. The use of attribute-based credentials in implementing Article 8 of the GDPR looks particularly promising, allowing for pseudonymous and reliable age checks online. In line with the risk-based approach embodied into the GDPR, methods of age verification that afford lower levels of assurance might be adequate in online services posing lower risks to the rights and freedoms of children, leaving high assurance options for high risk information society services, such as services involving profiling, marketing and other practises from which the GDPR considers that children merit specific enhanced protection.

When determining acceptable parental consent verification methods, the EU could follow the US example and encourage industry to propose effective, acceptable (from an industry perspective) and sector-tailored solutions for approval. Codes of conduct could be one possible

way to create standards for effective consent verification and the further specification of Article 8 of the GDPR. Nevertheless, in order to ensure that self-regulation is accountable, efficient and able to deliver on its societal goals, the EU should actively participate in the formulation of self-regulatory rules, and their effective monitoring and enforcement.

As regards the age threshold for consent, it might be worth adopting different age limits for different data collection areas and practises in the 13 to 16 year age span. Specific consent age limits could be determined in national laws as Member States can depart from the GDPR default age of 16 or in codes of conduct at the European level. The latter could help to create standards that account for children's vulnerabilities in a specific activity or sector. If the Member States chose to lower the age threshold to 13, the industry codes of conduct could still go beyond this age requirement and guarantee stringent protection in specific data collection scenarios offering more protection for children's personal data depending on the context. In any case, the choice of the most appropriate age limit between 13 and 16, be it in national law or in self-regulatory initiatives, should be based on extensive empirical evidence and consultations with children.

Chapter 4

Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law

Accepted to be published as a peer-reviewed book chapter:

Macenaite M., Protecting Children Online: Combining the Rationale and Rules of Personal Data Protection Law and Consumer Protection Law in Mackenrodt et al. (eds.) Personal Data in Competition, Consumer Protection and IP Law: Towards a Holistic Approach?, Springer, 2017 (forthcoming).

Abstract

The newly adopted EU General Data Protection Regulation (2016/679) has explicitly recognised that children deserve more protection than adults, especially online. Yet, as the GDPR's child-specific protection regime is new and without precedent in Europe, both its underlying logic and its practical implementation remain unclear. The chapter explores the extent to which EU consumer law, which has already taken account of children as a particularly vulnerable group of consumers, can inform the newly adopted General Data Protection Regulation. The analysis focuses on the reasons justifying the child-specific protection regime, principles (fairness, transparency) in relation to children and conceptual questions (definition of an average child and services directed to children).

Keywords: children, consumers, data subjects, data protection

1. Introduction

Children and young people are often at the forefront of grasping the new and exciting opportunities that the Internet can offer, such as playing, communicating, experimenting with relationships and identities, learning, creating and expressing themselves. It is estimated that globally one in three Internet users is under the age of 18.[335] In being both early adopters and active users of the Internet, children are also becoming increasingly influential as consumers, especially in the digital-content market.[336] A growing preference for online shopping rather than for brick-and-mortar stores can be observed in Europe, despite the lack of reliable and recent EU-wide data about children's expenditure on digital goods and services.[337] Young people using the Internet in particular show a big increase in online purchasing. In 2016, almost 70 percent of Internet users aged 16 to 24 in Europe had bought goods or services online.[338]

[335] Livingstone / Carr / Byrne (2015).
[336] Helberger / Guibault / Loos / Mak / Pessers / Van der Sloot (2013).
[337] The numbers of children purchasing, for example, apps online are significant. According to the European Commission (which cites an external study of Bitkom) only in Germany from 2012 to 2013 in-app purchases doubled amounting to 240 million EUR. More than one million of the app users were individuals aged between 10 and 19 years. European Commission (2014).
[338] Eurostat (2016).

Although the level of children's perception and attitudes towards online shopping varies and is influenced by many factors, such as age, parental guidance, social networks and peers,[339] and smaller children still might prefer physical over digital stores due to the variety of goods and instant gratification,[340] children undoubtedly as a consumer market have become very attractive for sellers and marketers. In fact, children are known to be a three-layer market: a primary market for their own purchasing power related to pocket money or income, an influence market, as children influence the buying patterns of their parents, and a future market, given their future spending power as purchasing habits and preference for brands continue into adulthood.[341]

Yet children are increasingly acting not only as consumers but also and at the same time as data subjects in their online activities. In the current data-driven information economy and the proliferation of the Internet of Things, almost any "smart" service or product comes with the collection of personal data and it is hard to imagine anyone being a consumer[342] without becoming a data subject (a natural person whose personal data is processed). As noted by Helberger et al., '(w)ith the integration of more and more data into consumer products, many data protection issues also become consumer issues, and vice versa'[343]. Consequently, there is a growing tendency to speak of consumers' rather than individuals' rights to data protection[344] and to look for an integrated vision of 'data consumer law'[345], reinforcing the close relationship between the roles of data subjects and consumers in the digital environment.

As '(p)ersonal data are economic assets, and are used to develop modern services, to categorise consumers, and to influence consumers'[346], the roles of consumers and data subjects are intertwined and the switch from the former to the latter can be hardly noticeable from a practical perspective. On a daily basis, consumers conclude agreements and consent to the collection of their data without necessarily fully realising that by simply ticking 'I agree' buttons on a website or adjusting device settings they consent to their data collection and use. For example, in order to create an account on social-networking sites, users accept the terms of use (virtually sign a legally binding contract as consumers) and consent to their personal data being processed by agreeing to the privacy policy of a site (act as data subjects).[347]

Widely spread business practices, such as combining contracts with consent (consent bundling)[348], when consumers allow collection and analysis of their personal data in addition to the provision of the main 'agreed' service, further contribute to blurring the line between consumers and data subjects and increase 'datafication',[349] which results in constant and opaque collection of consumers' personal data. In fact, the datafication of children's online activities is an increasingly growing research area, with studies examining digital dataveillance practices and their potential impact on children and their rights[350] and critically analyzing advertising, branding and marketing in games and apps directed towards children[351].

---

[339] Thaichon (2017).
[340] Boulay / de Faultrier / Feenstra / Muzellec (2014).
[341] McNeal (1999), 20; Buckingham (2000).
[342] Consumer is defined as 'any natural person who is acting for purposes which are outside his trade, business or profession' Article 2(b), Directive 93/13/EC.
[343] Helberger / Borgesius /Reyna (2017), 1428.
[344] Leczykiewicz / Weatherill (2016).
[345] Helberger / Borgesius /Reyna (2017), 1429.
[346] Ibid., 1430.
[347] Wauters / Lievens / Valcke (2015).
[348] Article 7(4) and Recital 43 of the General Data Protection Regulation (2016/679) create a presumption that consent bundling will render consent invalid as not 'freely given'.
[349] Mayer-Schönberger / Cukier (2013).
[350] Lupton / Williamson (2017)
[351] Grimes (2015).

Although the EU has paid specific attention to the vulnerability of children as consumers in the Directive 2005/29/EC on Unfair Commercial Practices[352], protection of children's informational privacy has been designed to conflate adults and children in one single group of data subjects. Since 1995, minors have been covered by the age-neutral data protection provisions of Directive 95/46/EC with no special focus on the processing of children's data, despite the fact that on a normative level, it is clearly acknowledged that a child's right to privacy needs to be considered separately from an adult's right to privacy.[353]

The newly adopted EU General Data Protection Regulation (2016/679)[354] (GDPR) has significantly changed the status quo and rejected the 'age-blind' approach to data subjects. For the first time, it explicitly recognises that children need more protection than adults, especially online, as 'they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data' (Recital 38). Such specific protection is afforded through a new two-tiered child-specific protection regime.[355] As the GDPR child-specific protection regime is new and without precedents in Europe,[356] both the underlying logic and the practical implementation of it remain unclear. For example, a lack of clarity exists about conceptual questions (definition of an average child and services directed to children) and principles (fairness, transparency) in relation to children.

The aim of this chapter is to explore the extent to which EU consumer law, which has taken account of children as a particularly vulnerable group of consumers, can inform the GDPR and reduce the clarity gap in relation to the above-mentioned GDPR concepts and principles.

The chapter is structured as follows. First, it defines consumers and data subjects in today's data-driven online environment and explores the legal qualification of the two roles in the case of children. It then examines the justifications for having a specific child-tailored data protection regime, going beyond the GDPR's obvious and explicit lack-of-knowledge yardstick. It broadens the view and takes into account the insights from social sciences on particular vulnerabilities and needs of children, as well as from consumer law and its legal vulnerability benchmark, partially embodying the social science insights. Finally, the chapter explores how consumer protection can inform data protection law by: 1) improving transparency through the information on data collection adapted to the specific needs and age of children; 2) enhancing fairness of data processing; 3) delineating services offered directly to

---

[352] Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive), 11.06.2005, L149/22.

[353] For example, Livingstone / Carr / Byrne (2015), 15 claim that '*greater steps are needed, because children's human rights necessitate special provision (special protection measures, best interest of the child, evolving capacity, participation, and so on), and there are good reasons to be concerned about whether children's rights will be met even where children and adults' rights are the same. This is because infringements of harm generally have a disproportionate impact on the vulnerable, and thus an approach that is age-generic (arguably, age-blind, by analogy gender-blind or disability-blind approaches) is unlikely to suffice*.'

[354] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), OJ L 119, 4.5.2016, 1–88.

[355] For a more detailed description of the two-tiered child-specific protection GDPR regime see Macenaite (2017).

[356] This regulatory effort is new for the EU, but the US almost two decades ago adopted detailed rules for the operators that collect personal information from children under the Children's Online Privacy Protection Act (COPPA). See Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505. For a detailed comparison between the requirements stipulated in the COPPA and the new rules in the EU see Macenaite / Kosta (2017).

children 4) defining an average child to decide when a child is able to provide a valid consent for the processing of his or her personal data.

2. Children as Data Subjects and Consumers Online: Defining Roles and Responsibilities

In the majority of the consumer law legal instruments 'consumer' is defined as a natural person who enters into a contract which falls outside his trade or profession.[357] This definition might prove problematic for adults. If interpreted in a narrow sense, it could catch individuals who use online services for both personal and professional purposes, for example send professional emails from their personal email accounts, store work-related documents on cloud storage services etc. This definition is less problematic for minors, who are rarely engaged in professional activities or trade.

However, a more relevant distinction for children is that between consumers and prosumers and between data subjects and data controllers. Children, in particular adolescents, actively take part in the collaborative or sharing economy and become co-creators of digital products and services. For example, they not only consume video games but also produce artefacts in the game-related affinity spaces,[358] not only watching but also creating and monetising digital content, such as videos, through advertising run on them on YouTube or blog posts through product endorsement and promotion. As technological developments and advancements, such as open design, additive manufacturing, crowd sourcing and open data, allow users to be a producer and a consumer at the same time, 'prosumer' as a legal concept escapes a clear legal definition, resulting in legal uncertainty about relevant rights and responsibilities. For example, when a third party (e.g. crowdsourcing platform) sells the co-created product and prosumers get part of the profit, an individual can be considered in a trade or business relation with the platform (i.e. producer) and might not be necessarily protected by consumer law in all cases.[359] Due to the unclear legal distinction between consumers, producers and prosumers, facts play a key role in courts when deciding if an individual qualifies as a consumer and 'the turnover, the amount of products, frequency or time involved in an activity of a prosumer helps to define in which quality a person acts'.[360] Also, due to the fact that consumers co-create their products or services, lack of clarity exists in relation to insurance coverage of potential accidents or the qualification of consumers when producing the goods and services.[361]

A similar shift is reflected in scenarios when Internet users change roles from data subjects to data controllers, losing the rights granted by data protection law. In line with its predecessor, the GDPR includes the 'household exception' (Article 2(c) GDPR). It clearly states that the Regulation 'does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity', such as social networking and online activity undertaken within the context of personal correspondence (Recital 18). However, the exact meaning of 'personal or household activity' is not entirely clear. The Court of Justice of the European Union (CJEU) in the *Lindqvist* case[362] concluded that the household exception is not applicable

[357] Article 2(b) of Unfair Contract Terms Directive, Article 2(a) of Unfair Commercial Practice Directive, Article 2(1) of Consumer Rights Directive.
[358] Wu (2016).
[359] Weitzenböck (2014), 487.
[360] Valant (2015), 16.
[361] Ibid.
[362] EU Court of Justice, Criminal proceedings against Bodil Lindqvist, C-101/01, ECLI:EU:C:2003:596, para. 46-58.

when information is accessible 'to an indefinite number of people', but the exact meaning of 'an indefinite number of people' lacks clarity. In the same vein, the Article 29 Working Party has acknowledged that a user 'may acquire a high number of third party contacts, some of whom he may not actually know' and this 'could be an indication that the household exception does not apply'.[363] As a result, the user who acts online and discloses personal data to a high or indefinite number of people could be considered a data controller and be obliged to comply with all the obligations stemming from the GDPR.

Such a provision no longer reflects the reality of today's data-driven online environment and expanded data processing capabilities of amateurs, and might have unintended consequences for social-network users.[364] Scholars have argued that it would be too burdensome to apply data protection rules to private individuals[365] and that supervisory authorities could not ensure compliance[366] and have noted even possible interference with individuals' fundamental right to privacy.[367]

On the other hand, excluded from the scope of data protection law harmed individuals would lose the possibility to lodge a complaint as data subjects and would need to opt for more burdensome civil-law actions (defamation, the right to protection of one's image) in courts.[368] Some potential solutions proposed, yet not directly implemented in the GDPR, include using a combination of five criteria to decide whether the household exemption applies to a particular processing activity: publicity of the disclosed data, types of data subject involved, scale and frequency of the processing, whether the activity is carried out singly or as a collective, and adverse impact.[369] Data protection authorities referring to these criteria would become more objective and gain a certain degree of discretion when deciding whether to take action in a specific situation.

When considering online behaviour, the application of data protection rules to children as data controllers appears to be theoretically probable even if undesirable. Empirical evidence suggests that adolescents have more contacts on social networks than adults or young adults and add more unknown people to contact lists simply as they want to know them or because they are popular or famous.[370] Networks of 'friends' tend to grow during the upper secondary school years and generally amount to approximately 500 contacts.[371] Given the conventional understanding of the data protection framework, it is unlikely that the finding children to be data controllers could be clearly excluded. However, as discussed below, the positioning of children as competent data subjects is already challenging and debatable and thus, the assignment of the complex duties and obligations imposed on data controllers may be even more problematic.

Nevertheless, from a theoretical perspective it is interesting to explore how data protection law could accommodate children as data controllers even if the household exemption did not apply. More specifically one could question whether a child could benefit from the exemption for the purposes of artistic or literary expression in the context of using a social network and thus how the balance between freedom of expression and the right to privacy could be struck in such circumstances. In addition, one could question how legitimate

[363] Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, WP 163, 2009.
[364] Helberger / Van Hoboken (2010) 103; Xanthoulis (2014).
[365] Garrie / Duffy-Lewis / Wong / Gillespie (2010).
[366] Wong / Savirimuthu (2008); Xanthoulis (2014).
[367] Article 29 Data Protection Working Party, Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities, 2013.
[368] Ibid.
[369] Ibid.
[370] Steijn (2014).
[371] Mantelero (2016).

interests as a condition for lawful processing in Article 6(1)(f) of the GDPR would be interpreted if a child is deemed to be a data controller and also how the 'legitimate grounds' for refusing the exercising of data subject rights could operate in practice. These abstract questions may have practical consequences and therefore may only be made clear via case law and CJEU interpretation. In the interim however doubt and room for abstract legal reasoning remain. As such, more research is required in this area.

2.1. Consumers of 'Free' Services?

Consumer protection has typically dealt with markets where products and services are traded in exchange of money. In fact, consumer rights have been traditionally guaranteed in sales and service contracts when the consumer pays a 'price', meaning payment in money, vouchers, gift cards or loyalty points with a specified monetary value rather than the services promoted by the trader as 'free'.[372] However, in the current data-driven information society the distinction between paid and 'free' electronic services has become obsolete both in theory and in practice. Paying not only with money but also with (personal) data for digital services and content has become an increasingly important way of bargaining online.

Such bargaining is particularly popular among younger Internet users, as various studies in Europe[373] and North America[374] report that the most favourite websites among children are those that do not require their users to pay for their services in terms of money, such as YouTube, Facebook and Google.

Although hidden costs of free services[375] and their detriment to consumers[376] have long been acknowledged by academics, the regulation of contracts in which a consumer 'pays' for a product or service by providing personal or other data to the supplier has been much slower.[377] Nevertheless, in its recent draft of a Directive on certain aspects concerning contracts for the supply of digital content (the proposed Digital Content Directive),[378] aiming to regulate digital content contracts such as downloading or web streamed of movies or digital services like cloud storage or social media, the European Commission has broadened the understanding of regular contract law, explicitly putting contracts in which the counter-performance refers to the payment of a price on equal basis with contracts where 'the consumer actively provides counter-performance other than money in the form of personal data or any other data' (Article 3(1)). Until this explicit acknowledgment of personal data as actual online currency, there were only sporadic references to this issue in several consumer-related EU guidance documents. The

---

372 European Commission, DG JUSTICE Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 13 June 2014 (hereinafter - Guidance Document concerning Directive 2011/83/EU).

373 Livingstone / Haddon / Görzig / Ólafsson (2011).

374 Steeves (2014a).

375 Bradshaw / Millard / Walden, (2011); Helberger / Guibault / Loos / Mak / Pessers / van der Sloot (2013); Loos / Luzak (2016).

376 Hoofnagle / Whittington (2016).

377 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (E-Commerce Directive) OJ L 178, 17.7.2000, p. 1–16, does not exclude information society services financed by advertising from its scope: *'information society services are not solely restricted to services giving rise to on-line contracting but also, in so far as they represent an economic activity, extend to services which are not remunerated by those who receive them, such as those offering on-line information or commercial communications, or those providing tools allowing for search, access and retrieval of data'* (Recital 18).

378 Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, 2015/0287 (COD).

European Commission's guidance document on unfair commercial practices refers to 'increasing awareness of the economic value of information related to consumers' preferences, personal data and other user-generated content'.[379] It stresses the importance of being transparent and informing consumers how their preferences, personal data and user-generated content are going to be used.[380] If consumers are not informed then the marketing of products that requires the exchange of personal data of users as 'free' could constitute a misleading practice.[381] Also, recently the Consumer Protection Cooperation Network in the social media context stressed that Directive 93/13/EC on Unfair Contract Terms is applicable to all types of contracts between consumers and businesses, explicitly mentioning as an example 'contracts where consumer generated content and profiling represent the counter-performance alternative to money'.[382]

Similarly, although without an explicit reference to personal data, the Directive 2011/83/EU on Consumer Rights (Consumer Rights Directive)[383] does not fully exclude 'free' online services from its scope and legal requirements. It distinguishes between sales and service contracts and contracts for the supply of online digital content.[384] Contrary to the definition of sales and service contracts, the Directive does not mention 'payment' for the digital-content contracts. Therefore, according to the European Commission, 'the Directive would seem to apply also to contracts for the supply of (…) online digital content even if they do not involve payment', such as the contracts for a free download of a game from an app store.[385] However, express contractual agreement needs to be concluded between consumers and traders and a mere access to a website is not necessarily considered a contract.[386] Therefore, 'contracts (for the supply of digital content in exchange of data) that are concluded by tacit agreement would escape the application of the Consumer Rights Directive'.[387]

That being said, it is unclear how this line of argumentation aligns with Article 5(3) of the ePrivacy Directive[388] which requires prior informed opt-in consent for storage and access to information on users' terminal equipment. It is uncertain how the collection of personal data via cookies for commercial purposes could be seen as a tacit agreement. In this regard, one could refer to the European Data Protection Supervisor's criticism of the proposed Digital Content Directive which delineates active and passive data collection despite the ePrivacy Directive's provisions.[389] Accordingly, there is a huge amount of debate and confusion surrounding a correct interpretation of the positioning of consent and its relationship with contract and contractual protections.

---

[379] European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final, 97.
[380] Ibid.
[381] Ibid.
[382] Consumer Protection Cooperation Network (2017), 3.
[383] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council Text with EEA relevance, OJ L 304, 22.11.2011, 64–88.
[384] It is not entirely clear how certain online services should be qualified: for example, should social-networking sites (SNSs) be considered as services or digital content? When the user signs up for a SNS he agrees to the terms of use or terms of service – a legally binding contract of service provision. The proposed Digital Content Directive, however, considers SNSs as being governed by provision-of-digital-content contracts.
[385] European Commission, Guidance Document concerning Directive 2011/83/EU, 8.
[386] Ibid, 64.
[387] Helberger / Borgesius /Reyna (2017), 1444.
[388] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (ePrivacy Directive), OJ L 201, 31.07.2002, 37 – 47.
[389] EDPS (2017).

In the same vein, the GDPR seems to hint that its scope extends to unpaid online services, i.e. to the processing of personal data when offering goods or services to data subjects in the EU, irrespective of whether a payment is required of the data subject (Article 3). Yet in Article 8 defining the conditions applicable to child's consent in relation to information society services the GDPR also explicitly refers to paid services, as information-society services are defined as 'any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services' (Point b of Article 1(1) Directive 2015/1535[390])). At first glance therefore it may seem that the reference to electronic services provided for remuneration requires direct remuneration from the users. However, in practice the phrase 'normally provided for remuneration' has been assigned a broad meaning. The CJEU has dealt with the concept of remuneration in various cases. It has ruled that the important element is that the remuneration is given to the provider of the service but it is not necessarily the recipient who has to give the remuneration. In *Belgium v Humbel* the CJEU considered that 'the essential characteristic of remuneration (…) lies in the fact that it constitutes consideration for the service in question'.[391] In *Bond van Adverteerders v Netherlands*, the CJEU found that the remuneration does not need to come from the recipient of the service, i.e. the viewer; it suffices that the remuneration comes from another party, such as an advertiser.[392] The CJEU has explained the concept of remuneration in the context of services offered within the European Union. It is unclear, however, if a service should be deemed distinct from a service contract, given that contract law remains largely dominated by national contract law vis-à-vis the requirements for contract formation.[393]

2.2. Legally (In)capable Consumers in (In)valid Consumer Contracts?

There is no clear definition of 'child' in the EU consumer law. The Unfair Commercial Practices Directive includes some provisions designed to protect children against unfair commercial practices, but does not specify who is a child. The guidance document mentions not only children but also teenagers as vulnerable consumers, but equally fails to provide concrete age ranges.[394] An interesting exception is the Toy Safety Directive,[395] where the concept of 'child' is linked to the notion of 'toy'. The Directive is applicable to 'products designed or intended, whether or not exclusively, for use in play by children under 14 years of age (hereinafter referred to as toys)' (Article 2.1).

Regulation or self-regulation fills this gap in certain cases on a national level. For example, the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing, adopted by the UK's Advertising Standard Authority, defines a child as an individual under 16.[396] In addition, as a general principle it acknowledges that 'the way in which children perceive and react to marketing communications is influenced by their age, experience and the context in which the message is delivered' and therefore, these factors are considered when examining whether specific marketing communication complies with the code. Interestingly,

[390] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, OJ L 241, 17.9.2015, 1-16.
[391] EU Court of Justice, Belgium v Humbel, C-263/86, ECLI:EU:C:1988:451, para. 17.
[392] EU Court of Justice, Bond van Adverteerders v Netherlands State, C-352/85, ECLI:EU:C:1988:196, para. 16.
[393] See Clifford / Van Der Sype (2016), 279-280.
[394] Commission Staff Working Document, Guidance on the Implementation /Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final.
[395] Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys, OJ L 170, 30.6.2009, 1.
[396] UK Advertising Standard Authority (2010).

the age threshold to become a data subject is much lower in the same code. Advertisers are allowed to collect personal data from children over 12 years old without parental consent.[397]

When defining a 'child' in consumer law, contract law is relevant to establish when a child may enter into contractual relations, but even contract law does not help in qualifying pre-contractual relations, such as product marketing or other commercial practices. In the majority of the national laws children are not considered legally capable to enter into valid contracts or do not have the competence to conclude agreements without parental permission. This prohibition follows from the assumption that minors are not fully capable of understanding the nature and legal consequences of their acts. Nevertheless, children between the ages of 14 and 18 in various jurisdictions are allowed to consent to agreements in small, day-to-day activities, such as those related to their income or daily life (e.g. buy food, clothes, transport tickets), without the involvement of their legal representatives.[398] For example, in Finland children under 15 can purchase only ordinary goods of small significance, such as spending their pocket money, without parental consent.[399]

The limits of the legal capacity to act online are much less clear. According to Wauters et al., actions of underage social-network users can have legal consequences if they can be qualified as 'daily acts' as well as if the minors are able to understand the scope of their actions (have reached the age of discernment).[400] A contract concluded by a minor who has not yet reached the age of discernment will be considered invalid or void.

The question of whether a minor can conclude a valid agreement online, e.g. accept the terms of service of a web-based service, should be answered according to the national contract law. For example, in Belgium a concluded standard contract is valid if the user has actual knowledge of the content of the contract and accepts the agreement.[401] Availability, visibility and comprehensibility of the contract terms are important, but the existence of actual knowledge has to be decided by a judge in a specific case.[402]

2.3. (In)competent Data Subjects?

Defining the 'legal competence' of children to consent to their personal data processing is a complicated task. Although the GDPR will mandate the establishment of clear age thresholds (leaving it to the Member States to define the precise age between 13 and 16 years), currently diverging age thresholds are explicitly introduced (or tacitly accepted in practice, depending on the Member State) for minors as data subjects while regulating their power to give valid consent to the data processing operations.[403] In general, many European countries consider minors of 14, 15 or 16 years as competent to consent to the processing of their data.[404]

A few national data protection laws in the EU explicitly state the exact age threshold from which minors are treated as legally competent to act as data subjects on their own behalf.[405] Other national legal frameworks do not include specific provisions, but rely on the

[397] Ibid.
[398] For a comparative overview of the legal capacity of minors in contract law see Loos / Helberger / Guibault / Mak / Pessers / Cseres / van der Sloot / Tigner (2011), 138-141.
[399] Finnish Competition and Consumer Authority (2015).
[400] Wauters / Lievens / Valcke (2015).
[401] Wauters / Lievens / Valcke (2015).
[402] Ibid.
[403] Macenaite / Kosta (2017).
[404] Dowty / Korff (2009).
[405] Parental consent is required for the processing of personal data of children under the age of 14 in Spain (Article 13 of the Spanish Royal Decree 1720/2007 of 21 December) and 16 in the Netherlands (Article 5 of

legal capacity of minors as actors in civil law or assess the concrete situation on a case-by-case basis.[406] In the latter case, the general criteria of the best interest of the child, the level of moral and psychological development, the capacity to understand the consequences of giving consent and evaluating specific circumstances (the age of the child, the purpose of data processing, type of personal data involved, etc) are taken into account in carrying out the assessment.[407] Such evaluation of the capacity of the data subject is a context-specific rather than universally applicable test, but assumption-based exemplary age thresholds are normally set in case law, legal doctrine or guidelines from the data protection authorities.[408]

3. Beyond the Obvious and Explicit: A Multitude of Raisons D'Être for a Specific Personal Data Protection Regime

The GDPR justifies its child-specific provisions exclusively in light of children's potentially lower awareness about the risks and safeguards related to the collection and use of their data. However, if the only reason for protecting children and young people was a lack of awareness, this problem could be addressed by intensive awareness-raising activities and would not necessarily require legislative action.[409] The following sections aim to explore the various additional factors which motivate the establishment of a specific, child-tailored data protection regime.

3.1. GDPR and the Lack-of-Knowledge Yardstick

The GDPR refers to children's lower awareness as a yardstick providing a normative justification for establishing its specific child-protection regime.

Lack of knowledge and of a full understanding of complex personal data-collection practices, along with their implications, especially online, is an undeniable problem not only for children and young people, but for many adults too. Research shows that some more advanced data-collection and tracking techniques, such as canvas fingerprinting and evercookies and their possible impact, are hard to understand even for sophisticated users.[410] Websites that are popular among children employ increasingly sophisticated methods to gather children's data as they play, communicate or browse online, resulting in constant surveillance. As Montgomery points out, the goal of these surveillance practices, used on many websites, is to create a cognitive, emotional and behavioral relationship between the child and the website,

---

the Dutch Personal Data Protection Act (25 892) of 23 November 1999) and Hungary (Section 6 (3) of the Hungarian Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information).

[406] Macenaite / Kosta (2017).

[407] Belgian Privacy Commission (2002); Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160; Dowty / Korff (2009).

[408] Macenaite / Kosta (2017).

[409] It should be acknowledged that effective awareness raising that leads to long term behavioural changes is not an easy objective to achieve. See Jones et al. (2013) for the analysis of online child safety education in the US.

[410] Acar / Eubank / Englehardt / Juarez / Narayanan / Diaz (2014).

through micro-targeted 'one-on-one' marketing and communication strategies.[411] Similar worries about the commercial surveillance of children in networked spaces, and the subsequent effects this may have, have been raised by a number of academics.[412]

For young people, privacy policies are long, complex, difficult to find and often age-inappropriate.[413] The privacy policies of the most widely used social-networking sites, such as Facebook and Twitter, can easily confuse users by valorising 'sharing' and 'control', despite the ongoing ubiquitous collection, use and disclosure of their data.[414]

Even though some children might be tech-savvy and informed Internet users, this does not necessarily render them capable of fully realising the consequences of pervasive online data-collection practices. For example, children do not intuitively perceive their online actions as actions that are being constantly monitored.[415] Even the mere positioning of children as 'digital natives'[416] or as part of 'the Net generation'[417] has been widely debated in the academic literature.[418] Empirical evidence suggests that other factors such as breadth of use, experience and education are in some cases even more decisive than generational differences in defining someone as a 'digital native'.[419]

3.2. Different Online Behaviour, Needs and Privacy Perceptions

The GDPR refers only to the (lack of) certain capacities pertaining to children rather than to the specific features characterising children, and especially adolescents, as individuals. Developmental psychology provides evidence that adolescents have particular needs and interests, such as identity formation, developing their agency and establishing autonomy, and creating peer relations.[420]

Making friends and forming peer relations become increasingly important with growth and can even affect the psychological, social and academic development of the adolescents.[421] Adolescents are eager to make new friends[422] and often establish more friendships than adults.[423] In contrast, young adults feel less need to engage in new friendships but more need to make the existing relationships more intimate and satisfying.[424] Adults spent less time with friends than do adolescents.[425] These claims are confirmed in the social-media context by several authors in Europe and beyond. In the Netherlands, Steijn and Schouten showed that younger social media users tend to create new relationships more often, while older users often strengthen ties with the existing friends.[426] In the same vein, Mantelero found that with increasing age adolescents in Italy consider it less important to look for new friends on social

411 Montgomery (2015).
412 Grimes (2015); Montgomery (2015); Rooney / Taylor (2017).
413 Micheti / Burkell / Steeves (2010); Grimes (2013).
414 Steeves (2017).
415 Savirimuthu (2016).
416 Prenksy (2001).
417 Tapscott (1998).
418 Helsper / Eynon (2010); Bennett / Maton / Kervin (2008).
419 Helsper / Eynon (2010).
420 Greenfield / Gross / Subrahmanyam / Suzuki / Tynes (2006); Subrahmanyam (2008); Subrahmanyam / Eddie / Harsono / Janice / Lawrence (2009).
421 Blieszner / Roberto (2004); Savin-Williams / Berndt (1990).
422 Boneva / Quinn / Kraut / Kiesler / Shklovski (2006).
423 Hartup / Stevens (1999); Blieszner / Roberto (2004).
424 Erikson (1968).
425 Hartup / Stevens (1999); Blieszner / Roberto (2004).
426 Steijn (2014), Steijn / Schouten (2013).

networks but rather communicate with the existing friends or family members.[427] The same trend is confirmed by Third et al. in relation to children from 16 countries around the world.[428]

Identity creation is an equally important need during adolescence.[429] Adolescents spend a lot of time with their peers, who become important circles where adolescent's identity is established.[430] Boneva et al. state that '[a]dolescence is defined by the need for intense person-to-person communication with a friend—spending a lot of time together ... and self-disclosing'.[431] Valkenburg and Peter show that the Internet social media have become a new arena for adolescents to present and experiment with their identities.[432] In contrast to children, older individuals have already developed their identities[433] and are willing to make them more solid and adults 'have less of a need to experiment with their identities or to present themselves favourably to others'.[434] Identity development and creation of relations as developmental needs are potentially connected with user online behaviour, such as adding contacts on their social networks and disclosure of personal information.[435]

Academics have established the link between developmental phases and online behaviour in relation to adolescents.[436] Empirical research also has elucidated that privacy perceptions and concerns are different between children, adolescents and adults. In particular, as claimed by Steijn, a developmental perspective can help to understand, and thus justify, the different privacy concerns and behaviour of individuals of different ages on social media.[437] Steijn relies on empirical evidence gathered in the Netherlands from 16 000 individuals in three age groups: adolescents (12- to 19-year-olds), young adults (20- to 30-year-olds) and adults (31-year-olds and older). He shows that behaviour of individuals on social media (e.g. having more contacts, posting information more frequently) can be related to characteristics that are typical for adolescents, young adults and adults in their life stages. Thus, developmental characteristics of relationship development and identity development are related to user behaviour on social media and can partially explain the lower concerns for privacy among adolescents.

3.3. Particular Vulnerabilities and Immaturities

The reliance on neurotechnology, in particular magnetic resonance imaging, in the last decade has provided neurological evidence to compare the different structures and functioning of adolescent and adult brains. Scientists have demonstrated that there are structural and functional immaturities in the brain of adolescents.[438] This has resulted in the questioning of Jean Piaget's previously dominant claim that by the age of 15, adolescents' cognitive capability to understand, appreciate, and articulate decisions are on par with those of an adult.[439] It has been instead acknowledged that 'teenagers may have the *ability* to reason like adults, but do so

[427] Mantelero (2016).
[428] Third / Bellerose / Dawkins / Keltie / Pihl (2014).
[429] Erikson (1959).
[430] Brown (1990), 179.
[431] Boneva / Quinn / Kraut / Kiesler / Shklovski (2006), 618.
[432] Valkenburg / Peter (2008).
[433] Waterman (1982).
[434] Steijn (2014), 51.
[435] boyd (2008); Boneva / Quinn / Kraut / Kiesler / Shklovski (2006); Mar wick / Diaz / Palfrey (2010); Peter / Valkenburg (2011).
[436] Peter / Valkenburg (2011).
[437] Steijn (2014).
[438] Giedd (2008); McAnarney (2008); McCreanor / Barnes / Gregory / Kaiwai / Borell (2005); Steinberg (2007, 2008).
[439] Cited in Preston / Crowther (2014), 454-455.

with vexing inconsistency'[440] due to, among others, their emotional volatility, impulsiveness, lower ability to deflect the pressure of peers.

Since the part of the brain controlling inhibitions fully matures only in early adulthood, adolescents can be less capable of evaluating risky situations and can be more easily misled. [441] They are less likely to consider the long-term consequences of their actions, and are more likely to be risk-prone.[442] As summarised by Preston and Crowther, '(n)otwithstanding growing research on the capabilities of teenagers and their need for respect and autonomy, the developmental science shows that, alongside these positive qualities, minors are nonetheless still impulsive, take more risks than adults, and are less capable of controlling their emotions' [443]. The authors continue: '(t)hese behavioral immaturities suggest that minors are not in the same position as adults when making long-term decisions, especially when surrounded by their peers' and further note that 'in the Internet age, they are always surrounded by their peers, using social media to bounce every decision off a host of other teenagers'[444].

These specific developmental features might influence their online behaviour and increase the possibility of online victimisation among peers, as well as the possibility of commercial personal data exploitation, to a level higher than that of cases involving younger children or adults. In the latter case, for example, online marketers can employ special strategies to take advantage of the adolescents' vulnerabilities, knowing that '[b]ecause of adolescents' emotional volatility and their tendency to act impulsively, they are also more vulnerable than adults to such techniques as real-time bidding, geolocation targeting (especially when an individual is near a point of purchase) and 'dynamic creative' adverts tailored to their individual profiles and behaviour patterns'.[445]

The manipulative and unfair techniques often used online to satisfy adolescent needs and the key features of online services that strongly meet adolescent needs have raised concerns among academics and policy makers.[446] As a result, the question has emerged whether certain data-collection practices with a potential negative impact that are directed to children, such as intrusive profiling or emotional manipulation, can be considered unfair and should be clearly prohibited in law, a question which will be discussed below.

3.4. Learning from Consumer Law – Vulnerability as a Legislative Benchmark

EU consumer law, in contrast to the data protection law, has already distinguished a special category of 'vulnerable consumers' and provided justification for their protection. Article 5(3) of the Unfair Commercial Practices Directive states: 'Commercial practices which are likely to materially distort the economic behaviour only of a clearly identifiable group of consumers who are particularly vulnerable to the practice or the underlying product because of their mental or physical infirmity, age or credulity in a way which the trader could reasonably be expected to foresee, shall be assessed from the perspective of the average member of that group.'

The Unfair Commercial Practices Directive creates a specific protection regime for vulnerable consumers as a special group because 'vulnerable consumers can be presumed to

[440] Ibid.
[441] Giedd (2008); McAnarney (2008); McCreanor / Barnes / Gregory / Kaiwai / Borell (2005); Steinberg (2007, 2008).
[442] Ibid.
[443] Preston / Crowther (2014), 454.
[444] Ibid.
[445] Montgomery (2015), 777.
[446] Montgomery (2015).

be in need of more protection than the "average consumer"'.[447] This regime provides enhanced protection departing from the general standard of consumer protection from unfair commercial practices, which is tailored to the average, 'reasonably circumspect' consumer. This approach, which Mak calls targeted differentiation, creates a criterion which follows specific needs of consumers in need of protection.[448]

This concept of vulnerability in the Unfair Commercial Practices Directive is essentially related to the personal situation of weakness in which individuals might find themselves due to their physical or demographic characteristics. The European Consumer Consultative Group calls this 'the personal dimension or horizontal approach' to consumer vulnerability.[449]

Although there exists no single, universally adopted definition of consumer vulnerability, the understanding of this concept in academic literature is much broader than in the Unfair Commercial Practices Directive. In addition to the personal characteristics of the consumer, increasingly more definitions include among vulnerability factors the overall situation in which the consumers find themselves. These factors can be divided into 'endogenous' (internal) and 'exogenous' (external) factors.[450] 'Endogenous' refers to 'causes that are inherent to the consumer or his or her physical or mental situation (children, adolescents, seniors, the disabled, etc.)'.[451] They can be temporary (e.g. illness) or permanent (e.g. impairment).[452] Exogenous causes include lack of knowledge of the language, lack of general or market-specific education or the need to use unknown new technologies.[453] Waddington claims that even 'the nature of the products', such as complex financial and investment products, or 'services and the selling arrangements', such as sales in combination with a free gift or special marketing practices, should count as external vulnerability factors.[454]

On the policy-making level as well, there have been calls to expand the definition of vulnerable consumers and incorporate 'situational vulnerability' or a 'sectoral approach'.[455] This approach would indeed recognise that the same consumers that in some markets are 'average consumers', i.e. reasonably well-informed, observant and circumspect, in other markets are vulnerable consumers who are not able to make informed, rational consumer choices.

Both groups of factors turn out to be important in practice. A recent empirical study on vulnerability demonstrates that the broader market environment is an important element of vulnerability, but that temporary or permanent characteristics of the consumer also play an important role.[456] Vulnerability can be both 'a permanent or long-term condition, often related to factors internal to the consumer, such as age, inexperience or a disability', and 'dynamic and relative' in its nature, arising in interaction with markets and services. Thus, any consumer can become vulnerable at times depending on his personal situation and characteristics and on the products or services and marketing used.[457] According to the European Commission's recent interpretation of the vulnerability concept, '[V]ulnerability is not a static condition. Consumers may move in and out of states of vulnerability and they may be vulnerable in respect of some

[447] Mak (2010).
[448] Ibid.
[449] European Consumer Consultative Group (2013).
[450] European Parliament, Report on a strategy for strengthening the rights of vulnerable consumers(2011/2272(INI)), 8 May 2012.
[451] Ibid.
[452] Ibid.
[453] Ibid.
[454] Waddington (2014).
[455] European Consumer Consultative Group (2013).
[456] European Commission, Consumer vulnerability across key markets in the European Union, Final report, January 2016.
[457] Waddington (2014).

categories of transaction but not others. In addition, vulnerability is best viewed as a spectrum rather than a binary state'.[458]

A recent EU study tried to provide an evidence-based definition of consumer vulnerability that can be used to update and enhance existing vulnerability definitions. According to the study, a 'vulnerable consumer' is:

> A consumer who, as a result of socio-demographic characteristics, behavioural characteristics, personal situation, or market environment:
> - Is at higher risk of experiencing negative outcomes in the market;
> - Has limited ability to maximise their well-being;
> - Has difficulty in obtaining or assimilating information;
> - Is less able to buy, choose or access suitable products; or
> - Is more susceptible to certain marketing practices[459]

This definition provides a comprehensive picture of vulnerability factors and resulting negative outcomes or limitations in consumer economic behaviour. It takes into account not only the demographic characteristics, such as age, and the market environment, but also behavioural features. In relation to children the latter is an important, albeit an often disregarded factor.

Personal factors, i.e. youth and consequently inexperience, are the primary causes of vulnerability. Youth is an enduring characteristic for this group of consumers. However, it could be claimed that children can be considered more vulnerable than many other types of consumers. While many other groups of consumers change their states of vulnerability by acquiring and losing external vulnerability factors, children will often fall under both groups of internal and external vulnerability factors. Children could be permanently vulnerable consumers due to their personal situation and often vulnerable due to the characteristics of products, services and marketing techniques.

3.5. Critical Understanding and Susceptibility

From a consumer law perspective, children and teenagers may be more vulnerable as consumers not only because they lack knowledge and skills, but also because (partially due of this lack) they can be more easily influenced by others.[460]

Research on consumer socialisation deals with the development of consumer skills, knowledge and attitudes of children and adolescents.[461] It indicates that the ability to act as consumers is increasingly acquired with growth. Research on the ability to understand advertising demonstrates that younger children are not able to identify, critically assess and understand the persuasive aim of advertising.[462] From 7 to 8 years of age children start to distinguish the persuasive intent and realise that advertisements can be deceptive or biased.[463] From 11 years children become more sceptical in relation to advertisements and their intent and tactics.[464] Rozendaal et al. specifically studied the differences in cognitive advertising competencies between children (8-12 years old) and adults (18-30 years old).[465] They showed that around the age of 9 to 10 children become able to recognise advertising to the same extent

[458] European Commission, Consumer vulnerability across key markets in the European Union, Final report, January 2016, xvii.
[459] Ibid., xx.
[460] Duivenvoorde (2013).
[461] John (2008).
[462] Martin (1997); Rozendaal / Lapierre / van Reijmersdal / Buijzen, (2011).
[463] John (2008).
[464] Ibid.
[465] Rozendaal / Buijzen / Valkenburg (2010).

as adults but at age 12 children still cannot understand selling and persuasive intent of advertising equally to adults.[466] Recognition of the selling intent of advertising develops earlier than the understanding of the persuasive intent.[467] Yet these age thresholds of recognising and understanding advertisements are not absolute or certain. Oates et al. claim that not all children who are 10 years old can understand the persuasive aim of advertisers.[468] Livingstone and Helsper show a more complex picture on the relationship between influence and age: 'different processes of persuasion are effective at different ages, precisely because literacy levels vary with age'.[469]

The findings on age ranges often reflect the research outcomes in the context of traditional advertising, such as on television or in newspapers, but are not to be directly transferred into the online context. Recognition of sophisticated advertising techniques in new media directed at children is much less explored than in traditional media. For example, there is only limited evidence on how children respond to embedded advertising on social media or advergames. The latter are particularly confusing due to the intrinsic intertwinement of commercial content and entertainment elements.[470] Even older children have difficulties in categorising advergames as entertainment or persuasion.[471] Their understanding even in later years of adolescence can be manipulated by advertisers through various covert techniques.[472] Product placement, host selling, branded websites and the use of celebrities all make it more difficult to understand the persuasive goal of marketing practices. A recent EU study confirms this conclusion by showing that although the most popular online games (of 25 studied games, all advergames, all social media games and half of the games provided through popular application platforms) contain embedded or contextual advertisements, children have difficulty in recognising the marketing intent of the content, in shielding themselves from it and in taking decisions.[473] The impact of imbedded advertising is considerable on children, subliminally changing their behaviour and purchasing decisions.[474]

Recent empirical data in the UK demonstrates the lack of critical understanding among children in the increasingly complex new-media landscape. Critical understanding is defined as 'a wide range of knowledge and skills, including the ability to make judgements about where information comes from and whether it is likely to be true' and 'awareness and understanding of advertising'.[475] Thus, the term describes the skills and knowledge children need to understand, question and manage online information and services. For example, only a small portion of surveyed 12- to 15-year-old children are able to identify sponsored links on Google as advertising (24% of 8- to 11-year-olds and 38% of 12- to 15-year-olds).[476]

[466] Ibid.
[467] Ibid.
[468] Oates / Blades / Gunter / Don, (2003), 69.
[469] Livingstone / Helsper (2006), 560.
[470] Rozendaal / Lapierre / van Reijmersdal / Buijzen, (2011); Verdoodt / Clifford / Lievens (2016).
[471] Fielder / Gardner / Nairn / Pitt (2008).
[472] Ibid.
[473] European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behavior, March 2016.
[474] Ibid.
[475] OFCOM (2016).
[476] Ibid.

4. Combining the Safeguards of the Personal Data and Consumer Protection Regimes… Benefiting Children?

The introduction of the specific child-related rules in the GDPR brings practical challenges in relation to the implementation of well-established but age-blind data protection principles, such as fairness and transparency. For example, data controllers in practice will have to figure out how to provide information about their data-collection practices to children in a meaningful way.[477] The GDPR child-specific rules also raise conceptual questions, such as how to define an average child and delineate services directed to children. Given that consumer protection law has dealt with children as vulnerable consumers, could it inform the application of data protection in the commercial context?

The answer to this question to a large extent depends on the agreement that consumer and data protection - despite their differences - can be matched as legal frameworks.[478]

At a first glance, the combination of consumer and data protection regimes seems rather intuitive. This is due to the fact that convergence between the two regimes is already happening in practice, in EU policy making and in EU law. As outlined above, the roles of consumers and data subjects are intrinsically intertwined in the digital environment, and therefore 'the protection of consumers' personal data is an integral part of consumer protection'[479]. On the EU policy level, the interrelation between data protection, competition law, and consumer protection in the Digital Economy has become an object of discussions introduced by the European Data Protection Supervisor.[480] The proposed Digital Content Directive acknowledged that consumers actually often pay for services not with money but with their personal data. The GDPR explicitly referred to the Unfair Terms Directive[481] in its Recital 42 when requiring the data controllers to provide intelligible and easily accessible pre-formulated declaration of consent without unfair terms and tackled other issues that are closely related to consumer protection, such as data portability. In addition to these convergences, more generally data protection and consumer protection share many common features: they are both recognised in the Charter of Fundamental Rights of the European Union (Article 8 (the right to data protection) and Article 38 (the consumer protection principle)[482], both are rooted in national laws of the Member States and developed as rights starting from bottom-up secondary EU legislation[483]. Both areas of law, generally, aim to protect weaker parties (consumers, data subjects) seen as often having asymmetric information and acting in an intrinsic power imbalance.

However, the interplay between consumer protection and data protection presents many challenges and the debate about these challenges is still in its nascent phase.[484] Despite their

---

[477] Savirimuthu (2016).

[478] For a comprehensive discussion about the match between consumer and data protection law and its positive and difficult sides see Helberger / Borgesius /Reyna (2017)

[479] Svantesson (2017)

[480] EDPS (2014)

[481] Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts (Unfair Terms Directive), OJ L 95, 21.4.1993, 29–34.

[482] Consumer protection is not as much fundamental substantive right at the EU primary-law level as data protection, but more a principle to be observed by public institutions, implemented through legislative or executive acts of the EU or the Member States and observed by the courts when interpreting these acts. Article 169 TFEU clearly outlines the objectives of the EU consumer-protection policy: protection of the health, safety and economic interests of consumers, promotion of their right to information and education and to organization in order to safeguard their interests.
Also, consumer rights are not human rights stricto sensu, although there have been efforts to argue that consumer rights should be considered (soft) human rights. See Deutch (1994).

[483] Svantesson (2017)

[484] Svantesson (2017), Helberger / Borgesius /Reyna (2017).

similarities, consumer and data protection pursue different goals, especially evident in terms of interests they protect. Consumer law essentially protects economic interests of consumers by regulating their relations with product and service providers and granting specific rights to consumers in economic transactions. Data protection law, instead, protects fundamental rights of individuals and strives for fairness and lawfulness when their personal data is processed. In short, '(c)onsumer law deals with fair contracting; data protection law with fair processing'.[485] This difference in goals also leads to additional complexities. For example, some of the underlying notions, such as fairness, damages or data, are not equivalent in data protection and consumer protection law and cannot be easily matched.[486]

Finally, and most importantly, conceptually there are some fundamental obstacles for merging consumer and data protection law. One of the main normative issues stemming from the differences in scope is that combining the rules of these two policy areas arguably necessitates assumption that personal data can be treated as property and reduced to a monetary value. Yet, as claimed by Helberger et al., 'fundamental rights, such as the right to privacy and to personal data protection, which also have a societal dimension, should not be downgraded to mere individual consumer interests'[487]. Therefore, 'neither laws nor policies should fuel the idea that people can renounce their rights in exchange of services'.[488] As a result, these concerns have to be addressed, or at least clearly explicated, before fully supporting the extension of consumer law rationales and rules into data protection, the area of fundamental human rights where personal data is much more than a commodity.

While acknowledging the differences between consumer protection and data protection and related conceptual challenges, it cannot be denied that the combination of the two areas can be informative and potentially enhance protection of children as data subjects and consumers in the data-driven digital world. Indeed, one must acknowledge the somewhat ironic oxymoronic consequences of failing to accept the economic significance of personal data as illustrated by the motivation behind the proposed Digital Content Directive to extend consumer protections. More specifically, although the EDPS has criticised the positioning of personal data as counter-performance[489], failing to do so also eliminates the proposed contractual protections where the only "price" paid is personal data thereby actually negatively impact the data subject's consumer rights and protections. Although the EDPS has recommended alternatives[490] in the opinion on the proposal, no clear solution has presented itself.

4.1. Child-Adapted Transparency

The GDPR requires data controllers to give information to all data subjects in a clear, audience-appropriate language when their personal data is collected. They are asked to adapt the information on data collection to children, as Recital 58 requires that information be given 'in such a clear and plain language that the child can easily understand'. In order to properly implement this requirement a change of mentality should happen, and data controllers should take account of the age, cognitive development, needs and abilities of the data subjects. As noted by Danoso et al.:

[485] Helberger / Borgesius /Reyna (2017), 1427.
[486] Ibid., 1460.
[487] Helberger / Borgesius /Reyna (2017), 1463.
[488] Ibid.
[489] EDPS (2017).
[490] In order to define the scope of the proposed Digital Content Directive without making reference to data as counter-performance, the EDPS recommended: 1) to use a broad definition of a 'service' in line with the E-commerce Directive, or 2) to refer (as the GDPR) to the offering of goods and services irrespective of whether a payment is required. EDPS (2017), 10-11.

> it is fundamental to re-think legal documents such as Terms of Use and Privacy Policies from a perspective that better fits children's needs, their rights and their not-yet fully developed cognitive capabilities. Increasing transparency in the case of children means communicating things differently, but openly, establishing clear boundaries regarding what is allowed on the website and what is not and, above all, relating the legal content as much as possible to the children's worldviews and experiences so that it becomes truly meaningful and engaging. Children are not adults, and therefore when it comes to legal communication, they should not be treated as such.[491]

In reflecting on a possible implementation of child-adapted transparency, personalised information, symbols and participatory transparency are considered as tentative solutions below.

4.1.1 Personalised Information

Consumer protection law has been based on the assumption that information asymmetry exists between service providers and consumers and that legislative obligations imposed on providers to make specific information available could correct the imbalance.[492] Therefore, presumably, if traders provide clear, accurate and substantiated information to consumers, consumers are enabled to make informed and meaningful choices. This information-based approach constituted 'the hallmark of EU consumer law' since the 1970s.[493] However, in recent years, drawing on the insights from behavioural economics, psychology and the neurosciences, this approach relying on the rational-choice model has been challenged as being no longer effective and reflecting neither consumer behaviour nor digital reality. Reliance on the average consumer as a yardstick contradicts empirical findings, and provision of standardised information is no longer able to restore symmetry between traders and consumers.[494] Thus, '"regulating for information" is passé and the new challenge is to 'regulate for rationality', or put more simply, to help consumers overcome cognitive biases that may be exploited by traders'.[495] As a consequence, alternative approaches replacing the information paradigm have been proposed, ranging from nudging[496] to personalised information disclosures.[497] The latter, invented by Busch, is particularly interesting in the case of children, although still at an early stage of academic debate. This approach proposes to use big-data analytics to provide personalised information disclosure to consumers instead of standard pre-contractual information, as currently prescribed by EU consumer law.[498]

Provision of such a personalised information theoretically looks very promising as it could take into account the specific needs, behaviour and vulnerabilities of consumers like children and tailor information to their age, personality, cognitive capacity. For example, based on past online behaviour, browsing history and demographic characteristics, algorithms could recognise a user as a child or even a child of a certain age and gender, and provide child-adapted information. The same logic and mechanism are employed by the behavioural advertising

[491] Donoso / van Mechelen / Verdoodt (2014), 54.
[492] Micklitz / Reisch / Hagen (2012), 272.
[493] Busch (2016).
[494] Sibony / Helleringer (2015).
[495] Ibid., 217.
[496] Sunstein (2014); Alemanno / Sibony (2015).
[497] Busch (2016).
[498] Ibid.

industry when serving targeted adds to the users, so could they be turned into the benefit of consumers?

Nevertheless, although promising and interesting from a consumer law perspective, personalised information as a transparency mechanism cannot be easily aligned with the core data-protection requirements. The implementation of this mechanism requires prior and potentially continuous personal data collection and profiling of children.[499] The GDPR allows measures based on profiling of adults with their explicit consent but limits the possibilities for profiling children, even if none of its articles explicitly states so. Recital 38 states that specific protection should apply when children's data is used for the purposes of creating personality or user profiles. Recital 71 instructs that solely automated decision-making, including profiling, with legal or similarly significant effects should not concern children. Yet recitals are not legally binding and cannot create rights and obligations that are not mentioned in the main legislative text.[500] Due to the lack of a clear position in the GDPR text, it can be debated whether the above-mentioned automated decisions are completely prohibited. The prohibition against creating personality or user profiles of children for targeted advertising purposes, for example, would be in line with the position of the Article 29 Working Party, which stated that behavioural advertising 'will be outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing'.[501] Even when profiling measures in relation to children are allowed by the GDPR, Article 22 of the GDPR will be interpreted strictly and in favour of children, for example, when deciding what decisions might have a significant effect on children.[502]

Nevertheless, in relation to personalised information as a transparency tool, it is questionable whether measures involving automated decisions based on profiling that aim to benefit children and enhance their rights, i.e. have no significant (negative) effect, should be allowed. If such measures were considered in line with the GDPR, what would be the legal ground for the related data processing? Would children be asked for explicit consent to be profiled, can such consent be informed and if so, at what age? If commercial profiling is allowed, even if for supposedly positive purposes, what additional safeguards can guarantee that the major problems associated with profiling, such as the lack of control over the profile, its possible use and abuse or opaque steering of consumer choices,[503] are accounted for?

4.1.2 Information in Symbols

The Consumer Rights Directive requires that information be provided in a 'clear and comprehensible manner'. The recitals of the Directive take particular account of vulnerable consumers, stating that the trader should take into consideration 'the specific needs of consumers who are particularly vulnerable because of their mental, physical or psychological infirmity, age or credulity in a way which the trader could reasonably be expected to foresee' (Recital 34). Not only the content of information is important, but also its presentation and

[499] In addition to the disproportionate data collection and processing, the EDPS also noted the following potential problem related to the automatic systems that infer the age of a user from his or her behavior: 'false identification of the age of the user under such behavioural analysis systems, particularly with respect to children who have a wide spectrum of maturity and behaviours as they grow and develop'. EDPS (2012), 7-8.
[500] Mendoza / Bygrave (2017).
[501] Article 29 Data Protection Working Party, Opinion 02/2013 on Apps on Smart Devices, WP 202, 27 February 2013.
[502] Mendoza / Bygrave (2017).
[503] Van der Hof / Prins (2008); Hildebrandt (2008).

visualisation.[504] Legal information for users should not only be as clear as possible, but also accessible and engaging. In fact, 'multi-layered' privacy notices[505] or visceral notices[506] have been proposed to improve the understanding and readability of information provided to the users. Visceral notices use intuitive, familiar visual signals in order to show consumers, instead of telling them, when their data is collected.

Although the GDPR has made its first steps in using symbols to improve transparency, icons have long been used in various sectors to inform consumers about products. Online digital products are not an exception, as the Guidance on the Consumer Rights Directive refers to the use of icons to provide information to consumers in a uniform and comparable way.[507] Its Annex I provides a set of icons to illustrate the relevant information categories, such as model for the display of consumer pre-contractual information about online digital products in accordance with Article 8(2) and (4) of the Consumer Rights Directive. It encourages traders to use the information categories with their icons.

The GDPR also mentions the use of standardised icons as easily visible and intuitive symbols for conveying privacy policies to the Internet users. Nevertheless, in the adopted text of the Regulation there is no effort to compose a list of such privacy icons. The European Parliament in its first reading provided a provisional list of icons and related particulars.[508] However, the list has been abandoned in the further GDPR adoption process and in practice has turned out to be controversial as to its comprehensiveness. This is not surprising, given that 'privacy safeguards are not easily reduced to metrics as are vitamins and calories on a nutritional label or miles per gallon on an auto sticker'.[509] In fact, research shows that representing privacy in icons is difficult, the icons are not always noticed by the users and the users need to learn the meaning of the icons, thus, user education is necessary in parallel.[510] Various icons have been developed by industry and academics, but their success has been limited.[511] For example, the AdChoices icon adopted by the online advertising industry has been seen as a failure as users had major troubles in understanding it.[512] However, it is also recognised that standard information mechanisms are necessary - although if used alone they are not sufficient – as such mechanisms help to find information more quickly and facilitate comparison among products and services.[513] For example, research found that a privacy "nutrition label" - a label inspired by actual nutrition labels used in food production - helped users to get information more accurately and quickly compared to traditional privacy policies.[514] Even if promising in research, this label has not yet been widely adopted in practice.

It is debatable if and to which extent icons, pictograms and other non-verbal ways of transmitting information can be effective and feasible for the implementation of the GDPR. In the light of empirical findings, it has been claimed that icons could provide a more intuitive

[504] John / Acquisti / Loewenstein (2009).
[505] Article 29 Working Party, Opinion 10/2004 on more harmonised information provisions, WP 100. Noain-Sánchez, (2015).
[506] Calo (2012), 1033.
[507] European Commission, Guidance Document concerning Directive 2011/83/EU.
[508] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 –C7-0025/2012 –2012/0011(COD)), P7_TA(2014)0212.
[509] Electronic Privacy Information Center (2012).
[510] Schaub / Balebako / Durity / Cranor (2015)
[511] See e.g., Disconnect Privacy Icons (at: https://disconnect.me/icons) or A. Raskin's Privacy icons (at: http://www.azarask.in/blog/post/privacy-icons/). Holtz / Zwingelberg / Hansen (2011).
[512] Leon / Cranshaw / Cranor / Graves / Hastak / Xu (2012).
[513] Cranor (2012).
[514] A privacy 'nutrition label' summarises main elements from a privacy policy in a standard form. See Kelley / Cesca / Bresee / Cranor (2010).

and easy to read privacy notices for children but traditional notices should remain available at the same time.[515] Indeed, the design and layout of visual notices, that might include not only images, icons but also text or the combination of all these elements, can influence users' attention and comprehension of the notice.[516] As younger children are less able to compare and select products and to deal with huge amounts of information when making decisions,[517] icons might turn out to be useful to them in finding and comparing information.

Notwithstanding the lack of effective solutions, the experience of consumer law can be inspirational for data protection law. For example, learning about the problems that the icons related to pre-contractual information about online digital products under the Consumer Rights Directive face could allow avoiding the same mistakes in data protection or help framing discussions about where changes are needed.

In the interim however not only the effectiveness of visual mechanisms to convey information to individuals should be increased but also adequate incentives should be put in place for the developed solutions to be adopted and enforced. Such an approach might better align the mismatch between the positive results in academic research versus the complete failure of self-regulatory transparency mechanism, such as the AdChoices icon. Moreover, definitive transparency mechanisms developed in collaboration with data protection authorities could create industry standards and common icons facilitating data subject awareness and allowing for the recognition of iconographic meaning.

4.1.3 Participatory Transparency

Even in child-adapted and easily readable or visualised privacy policies several discrepancies among users might remain, especially 'a gap between what users assume the terms contain and what they actually say' and the thinking among the users that terms and policies 'are there to protect them rather than consisting of a contract with legal obligations and duties'.[518] Empirical data on children demonstrates the existence of these cognitive biases. For example, 68 percent of Canadian children think that 'if a website has a privacy policy, that means it will not share my personal information with others'.[519] Similarly, in Italy many adolescents consider that 'the mere existence of a published privacy policy is *per se* sufficient to guarantee an adequate level of protection'.[520]

Instead of trusting that service providers will adapt their complex and legalese privacy policies to particular users and help to overcome the above-mentioned biases, user education and participation seems to be key in order to enhance transparency. Dreyer and Ziebarth propose relying on direct user engagement to improve transparency and readability of information that social-media services and platforms provide to their users.[521] More specifically, they suggest the participatory transparency approach, i.e. 'the use of autonomous bodies of third-party users to crowd-source platform-specific suggestions for improvements, and to translate terms and provisions into practical pointers'.[522]

---

[515] Mantelero (2016).
[516] Choe / Jung / Lee / Fisher (2013); Schaub / Balebako / Durity / Cranor (2015).
[517] John / Cole (1986).
[518] Dreyer / Ziebarth (2014), 532.
[519] Steeves (2014b).
[520] Mantelero (2016), 174.
[521] Dreyer / Ziebarth (2014).
[522] Ibid., 529.

The participatory transparency approach enables users to become active in explaining and transferring knowledge on the privacy policies and the terms of use to other users instead of being passive information receivers. In concrete terms, according to this approach, users can be organised in different forms ranging from formally institutionalised user boards and councils to informal forum and action groups. They are envisioned to contribute to the terms of use and privacy policies by unravelling their content and consequences, identifying problematic aspects and cognitive biases, demonstrating illegible and unclear provisions, aligning provisions with user expectations and social norms and providing crowd-sourced suggestions for improvements.[523] As proposed by Donoso et al., concrete mechanisms to realise this idea could be, for example, 'providing an *'idea-box'* for children to send suggestions about new (examples of) rules or agreements, or modifications to existing ones' or 'to develop a sort of "crowd-sourcing" feature where children can actively interact, discuss, propose and eventually vote on current and new rules'.[524]

The participatory transparency approach would not only make privacy policies of digital services and products more comprehensive, increase user awareness and possibly lead to improvements, but would also be aligned with the child-rights perspective. It would enable children to be heard and respect their rights to participate and express their views freely in all matters affecting them, as enshrined in Article 12 of the UN Convention on the Rights of the Child. Child participation means 'ongoing processes, which include information-sharing and dialogue between children and adults based on mutual respect, and in which children can learn how their views and those of adults are taken into account and shape the outcome of such processes'.[525] Meaningful participation and representation of children as Internet users can demonstrate their perspectives and values and contribute to the design of the rules that better resonate with children's viewpoints.

Improvement of transparency through the involvement of children has been used by scholars[526] and public institutions[527] studying the readability and comprehensibility of privacy policies within groups of children and exploring online privacy and transparency through youth juries.[528] Children's participation has proved to be particularly useful in identifying transparency issues, testing child-adapted privacy policies and deliberating and transferring knowledge about their implications.

4.2. Fairness

In addition to the duty of providing information to individuals, both data-protection and consumer protection law rely on the principle of fairness. Although it is challenging to combine the notions of fairness in both fields due to the potential differences in their scope and meaning, this is a necessary analysis in order to facilitate the alignment of these respective policy agendas.

[523] Ibid.
[524] Donoso / van Mechelen / Verdoodt (2014), 54.
[525] UN Committee on the Rights of the Child, *General Comment No. 12: The Right of the Child to be Heard*, UN Doc. CRC/C/GC/12, 20 July 2009.
[526] Micheti / Burkell / Steeves (2010); Donoso / van Mechelen / Verdoodt (2014).
[527] UK Children's Commissioner (2017).
[528] Coleman / Pothong / Perez Vallejos / Koene (2017).

4.2.1. Fairness in data protection

The GDPR, like its predecessor Directive 95/46/EC, requires data controllers to process personal data fairly. This principle generally enjoys a broad interpretation and means that personal data should be processed in a transparent way, i.e. data controllers are clear and open with data subjects about how and why their information will be collected and used. Besides transparent information, some interpret fairness as additionally requiring that personal data be handled only in ways individuals would reasonably expect, and most importantly, that personal data not be used in ways that unjustifiably cause a negative impact on individuals.[529] Bygrave claims: 'at a very general level, the notion of fairness undoubtedly means that, in striving to achieve their data-processing goals, data controllers must take account of the interests and reasonable expectations of data subjects; controllers cannot ride roughshod over the latter.'[530] There is a consensus among data protection authorities that 'any processing of personal data that gives rise to unlawful or arbitrary discrimination against the data subject shall be deemed unfair'[531].

Several authors have distinguished this broad role for fairness noting implicit and explicit meanings of the term. In particular, explicit fairness here strongly refers to transparency with implicit fairness relating instead to the balancing of interests and the reasonable expectations of the data subject.[532] In commenting on this division, Clifford and Ausloos instead propose a distinction between procedural fairness and fair balancing, given the modifications introduced by the GDPR in relation to fairness.[533] In short, the authors suggest a procedural fairness element composed of three components (namely transparency, timeliness and the burden of care) given the role played by data controllers in the implementation of the requirements.[534] In addition to this, the fair balancing elements relate to the principles of proportionality and necessity and their application to the balancing of the rights and interests in the context of the given circumstances.[535]

Due to the broadness of the overarching principle of fairness it is difficult to understand its precise meaning. As such, it is arguable that this principle could be informed by the fairness principle in consumer protection law (as contained in the Unfair Terms and Unfair Commercial Practices Directives).

4.2.2. Consumer protection and fair data gathering and use

Given that data protection is an omnibus regime, in consumer protection law the principle of fairness is more specific as it is restricted to the commercial business-to-consumer context. Fairness in consumer law refers not only to transparent contractual information, but also to the way in which a consumer is persuaded to agree to the contractual clauses and to the content of the clauses themselves. In short, there are two clear manifestations in fairness, namely: 1) the Unfair Terms Directive and 2) the Unfair Commercial Practices Directive.

The Unfair Terms Directive qualifies a non-negotiated term in a contract or a consent statement as unfair if, 'contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of

[529] ICO, the Guide to Data Protection (2016).
[530] Bygrave (2002), 58.
[531] International Conference of Data Protection and Privacy Commissioners, (2009).
[532] Bygrave (2002), Clifford / Ausloos (2017).
[533] Clifford / Ausloos (2017).
[534] Ibid.
[535] Ibid.

the consumer'.[536] Therefore, all contractual clauses are taken into account in determining unfairness, not limited to those related to the processing of personal data.[537]

The fairness test in the Unfair Terms Directive could be used to evaluate the fairness of terms and conditions related to personal data (e.g. excessive data collection, unlimited data sharing with the third parties) and the fairness of the position of the consumer in a commercial context. The fairness of contractual clauses could also be assessed using data protection requirements as an assessment criteria, e.g. a contract could be considered unfair if it violates data minimisation, security or data protection by default requirements.[538]

Consumer organisations have already referred to consumer law to test the fairness of the terms and conditions of companies collecting personal data. A recent example is an action which combined data protection and consumer protection to scrutinise the terms of use and privacy notices of connected toys.[539] Also in the context of social networks, the Unfair Term Directive has been applied to all types of contracts between consumers and businesses by the Consumer Protection Cooperation Network.[540]

Furthermore, the Unfair Commercial Practices Directive protects consumers from unfair commercial practices, i.e. any conduct by a trader directly connected with the promotion, sale or supply of a product, 'before, during and after a commercial transaction in relation to a product'.[541] As noted by Helberger et al., given that consent to personal data processing can be considered a transactional decision, the Unfair Commercial Practices Directive 'could help to assess the fairness of the conditions under which users are required to agree to the collection and use of their personal data – e.g. take-it-or-leave-it choices, misinforming about the functionality of the service if consumers do not agree, etc.'[542]

A practice is unfair if it is 'contrary to the requirements of professional diligence and materially distorts or is likely materially to distort the economic behaviour of the average consumer with regard to the product'.[543] Data processing practices that might have a detrimental effect on the average data subject, therefore, could be considered as violating the Unfair Commercial Practices Directive's fairness principle even if the data subject consented to them.

The use of consumer fairness test could have potential benefits for children and allow assessing them in the light of children's vulnerability to the practice or the underlying product. As outlined before, due to specific characteristics, needs and preferences children might be particularly vulnerable as consumers. For example, it has been argued that the use of certain techniques such advergames can have a manipulative effect with such techniques often implementing personal data gathering as part of the commercial offering.[544] Given the gamification of the personal data collection it is arguable that such a technique could fall foul of the fairness test in the Unfair Commercial Practices Directive. Interestingly, it is also questionable whether advergames themselves (i.e. aside from the data gathering aspects) may be in breach of the Unfair Commercial Practices Directive's fairness test due to the manner in which they integrate commercial and non-commercial content combined with the capacity to personalise such content.

[536] Article 3 of the Unfair Terms Directive.
[537] Wauters / Lievens / Valcke (2013), 64.
[538] Helberger / Borgesius /Reyna (2017), 1451.
[539] Forbrukerombudet (2016).
[540] Consumer Protection Cooperation Network (2017), 3.
[541] Article 2(k) and 3 of the Unfair Commercial Practices Directive
[542] Helberger / Borgesius /Reyna (2017), 1545.
[543] Articles 5(2) and 6(1)(a) of the Unfair Commercial Practices Directive.
[544] Verdoodt / Clifford / Lievens (2016)

Indeed, using personalised marketing 'companies could automatically adapt advertisements to (inferred) characteristics, biases and weaknesses of individual consumers'[545]. Thus, children's characteristics can be exploited by companies, taking advantage of their developmental features and manipulating their behaviour and decisions. A recent example of such manipulation is Facebook's ability to exploit emotional vulnerability of teenagers as allegedly 'the company can monitor posts and photos in real time to determine when young people feel "stressed", "defeated", "overwhelmed", "anxious", "nervous", "stupid", "silly", "useless" and a "failure"'[546] and allow advertisers to target ads accordingly.

Consumer law and its fairness principle could potentially address this concern. Relying on consumer protection, the GDPR could be interpreted as forbidding a priori some unfair and undesirable data collection and use (e.g. personalisation) practices. Consumer law would also allow to establish violation of fairness even in cases where the child or his representative has consented to the processing. In addition, the blacklist contained in Annex 1 in the Unfair Commercial Practices Directive could be updated to include a list of unfair commercial data-processing practices in order to ban them as misleading or aggressive, taking into account the aggressiveness, particular characteristics of children of differing age groups and the context. This would be in line with the thinking which has developed in the US after almost two decades of the COPPA experience. Montgomery and Chester argue that some collection practices of children's data, such as profiling, behavioral advertising, cross-platform tracking and geolocation targeting should not be allowed by law even with parental permission.[547]

Yet, the impact of these suggestions should be carefully considered in light of the UN Convention on the Rights of the Child, which in addition to protection provide children with strong claims related to participation and provision.[548] A blunt prohibition of specific data collection practices could be viewed as overprotection for older children, who (if properly informed) might be increasingly able to decide for themselves to consent to such practices or not. However, the limitations and shortcomings of consent are widely acknowledged in relation to adults, let alone children.[549] Also, many data processing practices might not be easily classified as having a purely negative effect and might in parallel bring some benefits for a child, which can easily be curtailed by taking too paternalistic approach. Despite this, one must acknowledge that the very purpose of many of these practices is to manipulate.

Therefore, reliance on fairness as it is understood in consumer protection law could allow data protection to shift the focus from procedural safeguards (e.g. parental consent to data processing) to a fundamental and comprehensive assessment of data processing practices and terms as fair.[550]

4.3. Services Offered Directly to Children

The GDPR requires parental consent when online services are offered directly to children under the age of 16 (unless national laws specify a lower age threshold between 13 and 16). However, websites with mixed audiences rather than services created for children are the ones

[545] Helberger / Borgesius /Reyna (2017), 1458.
[546] The Guardian, Facebook told advertisers it can identify teens feeling 'insecure' and 'worthless', 1 May 2017, available at: https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens
[547] Montgomery / Chester (2015).
[548] Article 12 (the right to be heard) and Article 17 (the right to have access to media) of the UN Convention on the Rights of the Child.
[549] Van der Hof (2016).
[550] On the limits of protection offered to children under the rules on children's consent in the EU see Van der Hof (2016).

to generate major privacy concerns and anxieties. Various studies in Europe[551] and North America[552] report that from a broad range of websites that children nowadays use, the most favorite websites are often not directed to or targeting children (at least not those under 13), such as YouTube, Facebook and Google. Many of these websites claim in their terms of use that their services are not intended for those under 13, even if in practice young children are active there in substantive numbers. It is well documented that services not directed or clearly appealing to children, e.g. contain no cartoon characters, are used by children.[553]

Due to the very recent GDPR adoption, there has been no official guidance at the EU level on the extent that the parental-consent requirement will cover general-audience or mixed-audience services and sites. Therefore, many uncertainties and questions remain: How to delineate information-society services offered directly to a child from general-audience services? How many children should the service have among its users to be covered by the GDPR parental-consent requirement, i.e. what if it does not target children as its primary audience? When, if at all, does the GDPR apply to mixed-audience websites? Do data controllers need to have 'actual knowledge' that children are providing them with personal data?[554]

The Unfair Commercial Practices Directive entails a similar difficulty to distinguish marketing directed at children from marketing directed at other consumers and could become a useful reference in the GDPR implementation process. In order to decide whether marketing is directed at children, the European Commission requires a case-by-case assessment, which should not be limited to the trader's target-group definition.

In interpreting the application of Article 5(3) and (5) and point No. 28 of Annex I to the Unfair Commercial Practices Directive to games, the European national consumer protection authorities, acting through the Consumer Protection Cooperation (CPC) Network, took the position that the Unfair Commercial Practices Directive applies not only to games 'solely or specifically targeted at children', but also to games that are 'likely to appeal to children'.[555] The trader should be reasonably able to foresee that his service is likely to appeal to children.[556]

In addition, national authorities have adopted criteria to determine whether services are likely to appeal to children. For example, the Principles for online and app-based games developed by the UK Office of Fair Trading establish the following open list of criteria related to the content, style and presentation of the game: characters popular with children, cartoon-

[551] Livingstone / Haddon / Görzig / Ólafsson (2011).
[552] Steeves (2014a).
[553] Consumer Protection Cooperation Network (2013).
[554] The Federal Trade Commission (FTC) under the COPPA in the US takes into account the following for determining whether a website or an online service is directed at children: subject matter of the site, its visual content, the use of animated characters or child-oriented activities and incentives, music or other audio content, age of models, presence of child celebrities. A service will not be considered by the FTC to be directed to children if it does not target children as its primary audience and employs a filter ensuring that personal information from users is not collected prior to ascertaining their age, and consequently prevents the collection of personal information from individuals who have stated they are younger than 13. See FTC, A Guide for Business and Parents and Small Entity Compliance Guide, available at: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions
[555] Consumer Protection Cooperation Network (2013), 2. (It states: '*As to whether an application or a game can be considered to be directed at children within the meaning of Annex I Nr 28, the UCPD (Unfair Commercial Practices Directive) gives no clear indication. Other provisions in the UCPD contain useful criteria which can be used mutatis mutandis to address this matter. For example, Article 5(2)(b) refers to the distortion by a practice of the economic behaviour of the consumer whom it "reaches". Similarly, under Article 5(3), where a clearly identifiable group of consumers is particularly vulnerable to a practice in a way which the trader could reasonably be expected to foresee, the practice shall be assessed from the average member of that group'*)
[556] Ibid.

like graphics, bright colours, simplistic language, activity appealing to or popular among children, no age restriction for downloading, availability in the child section in an app store.[557]

The guidance for data controllers on the definition of information-society services offered directly to a child could take into account the Unfair Commercial Practices Directive's interpretation of marketing directed at children and include services that are likely to appeal to children due to their content, style and presentation and services actually used by children (based on e.g. empirical evidence on audience composition), even if the service provider employs a different target-group definition.

4.4. Defining an Average Child

When a commercial practice is specifically aimed at a particular group of consumers, such as children, the Unfair Commercial Practices Directive advises that the impact of the commercial practice be assessed from the perspective of the average member of that group. The average-consumer standard, although criticised as imprecise and ambiguous,[558] is dynamic. National courts and authorities have to exercise their own discretion and judgment and determine the typical reaction of the average consumer in a particular case. According to Mak, 'the "unfair" character of advertising is determined on the basis of consumer perception' and the risk of 'consumer confusion' is a touchstone for the applicability of the Unfair Commercial Practices Directive.[559]

If a commercial practice is targeting a group of consumers who are less than averagely informed and circumspect, the average member of that group (rather than the average consumer in general) should be taken as the standard of assessment. For example, in advertising for children, the consumers addressed are potentially less critical and less knowledgeable of influencing practices, leading to a stricter evaluation of the advertising involved.[560]

The Unfair Commercial Practices Directive implicitly requires examining the age of the group of children targeted by the commercial practice, and determining whether this age group is vulnerable to the practice at hand. The GDPR also relies on an average-child criteria when providing protection to children as data subjects through parental consent. However, instead of evaluating an average child of a particular targeted age group, the GDPR chooses to set an age when children can be deemed competent to consent to the processing of their personal data. Such a legislative choice of determining a prescribed age limit does not account for particular age groups, their vulnerability to the particular data-collection practice or their perception.

Data-protection law could therefore define an average child in different data-collection scenarios based on comprehensive research and solid empirical evidence. As it seems highly unlikely that fixing a single age limit for consent in all data-processing activities online could be the most appropriate solution, different sectors, data-collection practices and age spans might require detailed examination and research.

Following the logic of the Unfair Commercial Practices Directive, the GDPR could start searching for an average data subject among children and explore the correlation between the characteristics of certain age groups of children and their likelihood of being vulnerable for specific commercial data-collection practices.[561]

---

[557] Office of Fair Trading (2014).
[558] Incardona / Poncibò (2007), 21.
[559] Mak (2010).
[560] Duivenvoorde (2013).
[561] Stuyck / Terryn/ van Dyck (2006).

5. Conclusions

When trying to solve the new data-protection challenges pertaining to the child-specific protection regime of the GDPR, the EU data-protection law should not try to invent the wheel but combine its efforts with consumer protection law. A holistic view on the rationale and particular provisions of both fields would not only provide inspiration from consumer law, which has been dealing with children as vulnerable consumers for some time, but also reflect the dual role of data subjects and consumers that children today play online.

In the GDPR, children, as a specific group of data subjects, are considered separately from adults because of their possible lower awareness of risks, consequences, safeguards and rights in relation to the processing of personal data online. However, the need for more protection stems from various additional factors which did not evidently motivate the European Commission. This chapter aims to broaden the understanding of the normative justifications for establishing a specific, child-tailored two-tiered data protection regime. It has showed that EU consumer protection law portrays children as vulnerable consumers due to their possible susceptibility to advertising and manipulation by traders and marketers. Both internal (e.g. age) and external (e.g. complex products and data-driven markets) elements contribute to such vulnerability. Not less important are specific interests of persons who have not yet reached physical, psychological and intellectual maturity and need to freely develop into adults. Developmental psychology underlines specific developmental features, such as emotional volatility and impulsiveness, need of identity and autonomy formation that can increase the possibility of online victimisation and commercial exploitation of personal data among children.

The chapter has also demonstrated that the GDPR can learn from consumer law in implementing child-adapted transparency, for example through participatory transparency and icons, and broadening the understanding of the fairness principle and as a result banning data collection practices that are contrary to good faith and might have detrimental effects on children as data subjects. Consumer law can provide guidance on how to interpret the definition of information-society services offered directly to a child, making it possible to include not only services directly targeting children but also those that are likely to appeal to children due to their content, style and presentation. Finally, following the logic of the Unfair Commercial Practices Directive, the GDPR could rely on an average data subject, define an average child in different data collection scenarios and explore the correlation between the characteristics of certain age groups of children and their likelihood of being vulnerable to specific commercial data collection practices.

References

Acar, G. / Eubank, C. / Englehardt, S. / Juarez, M. / Narayanan, A. / Diaz, C. (2014), The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, In Proceedings of CCS 2014, available at: https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf.

Alemanno, A. / Sibony, A. L. (2015), Nudge and the Law: a European Perspective, Hart Publishing.

Bennett, S. / Maton, K. / Kervin, L. (2008), The 'digital natives' debate: A critical review of the evidence, 39 British Journal of Educational Technology 775.

Blieszner, R., / Roberto, K. A. (2004), Friendship across the life span: reciprocity in individual and relationship development, in: F.R. Lang / K.L. Fingerman (eds.), Growing together: personal relationships across the lifespan, 159–182. Cambridge, UK: Cambridge University Press.

Boneva, B.S. / Quinn, A. / Kraut, R.E. / Kiesler, S., / Shklovski, I. (2006), Teenage communication in the instant messaging era, in: R. Kraut / M. Brynin / S. Kiesler (eds.) Computers, phones, and the Internet: Domesticating information technology, 201-218. Oxford, New York: Oxford University Press.

Boulay, J. / de Faultrier, B. / Feenstra, F. / Muzellec, L. (2014), When children express their preferences regarding sales channels: Online or offline or online and offline?, 42 (11/12) International Journal of Retail & Distribution Management, 1018.

boyd, D. M. (2008), Taken out of context: American teen sociality in networked publics. PhD thesis, University of California, Berkeley.

Bradshaw, S. / Millard, C. / Walden, I. (2011), Contracts for clouds: Comparison and analysis of the terms and conditions of cloud computing services, 19 International Journal of Law and Information Technology 187.

Buckingham, D. (2000). After the Death of Childhood, Cambridge, Polity.

Busch, C. (2016). The Future of Pre-Contractual Information Duties: From Behavioural Insights to Big Data, in: C. Twigg-Flesner (ed.), Research Handbook on EU Consumer and Contract Law, 221-241, Edward Elgar Publishing.

Bygrave, L. A. (2002), Data Protection Law: Approaching its Rationale, Logic and Limits, Kluwer International: Den Haag, 2002.

Calo, R. (2012), Against Notice Skepticism In Privacy (And Elsewhere), 87 Notre Dame Law Review 1027.

Choe, E. / Jung, J. / Lee, B. / Fisher K (2013). Nudging people away from privacy-invasive mobile apps through visual framing. In Proc.INTERACT'13. Springer.

Clifford, D. / Ausloos, J. (2017), Data Protection and the Role of Fairness, CiTiP Working Paper 29/2017, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3013139

Clifford, D. / Van Der Sype, Y.S. (2016), Online dispute resolution: Settling data protection disputes in a digital world of customers, Computer 32(2) Law & Security Review 272.

Coleman, S. / Pothong, K. / Perez Vallejos, E. / Koene, A. (2017), Internet On Our Own Terms: How Children and Young People Deliberated About Their Digital Rights, available at: http://casma.wp.horizon.ac.uk/casma-projects/5rights-youth-juries/the-internet-on-our-own-terms/

Cranor, L. F. (2012), Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, 10(2) Journal on Telecommunications and High Technology Law 307.

de Zwart, M. / Lindsay, D. / Henderson, M. / Philips, M. (2001), Teenagers, legal risks & social networking sites, available at: http://newmediaresearch.educ.monash.edu.au/moodle/pluginfile.php/2117/mod_label/intro/SNSandRisks_REPORT.pdf

Deutch, S. (1994), Are consumer rights human rights?, 32(3) Osgoode Hall Law Journal, 537.

Donoso, V. / van Mechelen, M. / Verdoodt, V. (2014), Increasing User Empowerment through Participatory and Co-design Methodologies, Emsoc project deliverable D1.3.1c, available at: http://emsoc.be/wp-content/uploads/2014/09/D1.3.1c_ICRI1.pdf

Dowty, T. / Korff, D. (2009), Protecting the virtual child – the law and children's consent to sharing personal data, Study prepared for ARCH (Action on Rights for Children) and the Nuffield Foundation, available at: http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf

Dreyer S. / Ziebarth L. (2014), Participatory Transparency in Social Media Governance: Combining Two Good Practices, 4 Journal of Information Policy 529.

Duivenvoorde, B. (2013), The protection of vulnerable consumers under the Unfair Commercial Practices Directive, 2 Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht 69.

Erikson, E.H. (1959), Identity and the life cycle. New York: Norton.

Erikson, E.H. (1968), Identity: youth and crisis. New York: Norton.

Fielder, A. / Gardner, W. / Nairn, A. / Pitt, J. (2008), Fair Game? Assessing commercial activity on children's favourite websites and online environments, UK National Consumer Council.

Garrie, D. B. / Duffy-Lewis, M. / Wong, R. / Gillespie, R. L. (2010), Data Protection: the Challenges Facing Social Networking, 6 Brigham International Law and Management Review, 127.

Giedd, J.N. (2008), The Teen Brain: Insights from neuroimaging, 42 Journal of Adolescent Health 335.

Greenfield, P.M. / Gross, E.F. / Subrahmanyam, K. / Suzuki, L.K. / Tynes, B. (2006), Teens on the Internet: Interpersonal connection, identity, and information, in: R. Kraut (ed.), Information technology at home, 185-200, Oxford University Press.

Grimes, S.M. (2013), Persistent and emerging questions about the use of end-user licence agreements in children's online games and virtual worlds, 46 UBC Law Review 681.

Grimes, S.M. (2015), Playing by the Market Rules: Promotional Priorities and Commercialization in Children's Virtual Worlds, 15 Journal of Consumer Culture 110.

Hartup, W.W. / Stevens, N. (1999), Friendships and adaptation across the life span, 8(3) Current Directions in Psychological Science 76.

Helberger, N. / Borgesius, F. Z. / Reyna, A. (2017), The perfect match? A closer look at the relationship between EU consumer law and data protection law, 54(5) Common Market Law Review, 1427.

Helberger, N. / Guibault, L. / Loos, M. / Mak, C. / Pessers L., Van der Sloot, B. (2013), Digital Consumers and the Law. Towards a Cohesive European Framework, Kluwer Law International.

Helberger, N. / Van Hoboken, J. (2010), Little Brother Is Tagging You –Legal and Policy Implications of Amateur Data Controllers, 4 Computer Law International 101.

Helsper, E.J. / Eynon, R. (2010), Digital natives: where is the evidence?, 36 British Educational Research Journal 503.

Hildebrandt, M. (2008), Defining Profiling: A New Type of Knowledge?, in: M. Hildebrandt / S. Gutwirth (eds.), Profiling the European citizen Cross-disciplinary perspectives, 17-45, Den Haag: Springer Science.

Holtz, L. E. / Zwingelberg, H. / Hansen, M. (2011), Privacy Policy Icons, in: J. Camenisch, S. Fischer-Hübner, K. Rannenberg (eds.) Privacy and Identity Management for Life, 279-285, Springer-Verlag GmbH Berlin.

Hoofnagle, C. J. / Whittington, J. (2016), The Price of 'Free': Accounting for the Cost of the Internet's Most Popular Price, 61 UCLA law review 606.

Incardona, R. / Poncibò, C. (2007), The average consumer, the Unfair Commercial Practices Directive, and the cognitive revolution, 30 Journal of Consumer Policy 21.

John, L. / Acquisti, A. / Loewenstein, G. (2009), The Best of Strangers: Context Dependent Willingness to Divulge Personal Information, available at: http://ssrn.com/abstract=1430482.

John, R. D. (2008), Stages of consumer socialization, in: C. P. Haugtvedt / P. Herr / F. R. Kardes (eds.), Handbook of consumer psychology, 219–226, New York: Taylor & Francis.

John, R. D. / Cole, C. A. (1986), Age Differences in Information Processing: Understanding Deficits in Young and Elderly Consumers, 13 Journal of Consumer Research 297.

Jones, L. M. / Mitchell, K.J. / Walsh, W. A. (2013), Evaluation of Internet Child Safety Materials Used by ICAC Task Forces in School and Community Settings: NIJ Evaluation Final Technical Report, Washington, DC.

Kelley P.G. / Cesca, L. / Bresee, J. / Cranor L.F. (2010), Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach, CYLAB, available at: http://www.cylab.cmu.edu/research/techreports/ 2009/tr-cylab09014.html.

Leczykiewicz, D. / Weatherill, S. (2016), The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law, Hart Publishing.

Leon, P. G. / Cranshaw, J. / Cranor, L.F./ Graves, J. / Hastak, M. Ur, B. / Xu, G. (2012), What do online behavioral advertising privacy disclosures communicate to users? In Proc.WPES'12.ACM.

Livingstone S. / Helsper, E. J. (2006), Does advertising literacy mediate the effects of advertising on children? A critical examination of two linked research literatures in relation to obesity and food choice', 56(3) Journal of Communication 560.

Livingstone, S. / Carr, J. / Byrne, J. (2015), One in Three: Internet Governance and Children's Rights, Global Commission on Internet Governance Paper Series No. 22, London: Centre for International Governance Innovation.

Livingstone, S. / Haddon, L. / Görzig, A. / Ólafsson, K. (2011), Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries, EU Kids Online, Deliverable D4, EU Kids Online Network.

Loos M. / Helberger, N. / Guibault, L. / Mak, C. / Pessers, L. / Cseres, K. J. / van der Sloot, B. / Tigner, R. (2011), Final report Comparative analysis, Law & Economics analysis, assessment and development of recommendations for possible future rules on digital content contracts, available at: http://ec.europa.eu/justice/consumer-marketing/files/legal_report_final_30_august_2011.pdf

Loos, M. / Luzak, J. (2016), Wanted: A Bigger Stick, On Unfair Terms in Consumer Contracts with Online Service Providers, 39(1) Journal of Consumer Policy 63.

Lupton, D. / Williamson, Ben. (2017), The datafied child: The dataveillance of children and implications for their rights, 19(5) New Media & Society 780.

Macenaite, M. (2017), From universal towards child-specific protection of the right to privacy online: dilemmas in the EU General Data Protection Regulation, 19 (5) New Media and Society 765.

Macenaite, M. / Kosta E. (2017), Consent for processing children's personal data in the EU: following in US footsteps?, 26(2) Information & Communications Technology Law 146.

Mak, V. (2010), Standards of Protection: In Search of the 'Average Consumer' of EU Law in the Proposal for a Consumer Rights Directive, 1 European Review of Private Law 8.

Mantelero, A. (2016), Children online and the future EU data protection framework: empirical evidences and legal analysis, 2(2–4) International Journal of Technology Policy and Law 169.

Martin, M. C. (1997), Children's understanding of the intent of advertising: A meta-analysis, 16 Journal of Public Policy and Marketing 205.

Mayer-Schönberger, V. / Cukier, K. (2013), The Rise of Big Data: How it's Changing the Way We Think about the World, 92 Foreign Affairs 28.

McAnarney, E.R. (2008), Adolescent Brain Development: Forging New Links?, 42 Journal of Adolescent Health 321.

McCreanor, T. / Barnes, H.M. / Gregory, M./ Kaiwai, H. / Borell, S. (2005), Consuming identities: Alcohol marketing and the commodification of youth experience, 13 Addiction Research & Theory 579.

Mendoza, I. / Bygrave, L. A. (2017), The Right Not to Be Subject to Automated Decisions Based on Profiling, in: Synodinou, T. / Jougleux, P. / Markou, C. / Prastitou T. (eds), EU Internet Law: Regulation and Enforcement, Springer.

Micheti, A. / Burkell, J. / Steeves, V. (2010), Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand, Bulletin of Science, 30 Technology & Society 130.

Micklitz, H. W. / Reisch, L. / Hagen, K. (2012), An Introduction to the Special Issue on "Behavioural Economics, Consumer Policy, and Consumer Law", 34 Journal of Consumer Policy 272.

Montgomery, K. C. (2015), Youth and surveillance in the Facebook era: Policy interventions and social implications, 39 Telecommunications Policy 771.

Montgomery, K. C. / Chester, J. (2015), Data protection for youth in the digital age: Developing a rights-based global framework, 1 European Data Protection Law Review 291.

Noain-Sánchez, A. (2015), ""Privacy by default" and active "informed consent" by layers: Essential measures to protect ICT users' privacy." Journal of Information, 14 (2) Communication and Ethics in Society 124.

Oates, C. / Blades, M. / Gunter, B. / Don, J. (2003), Children's understanding of television advertising: a qualitative approach, 9 Journal of Marketing Communications 59.

Peter, J., / Valkenburg, P. (2011), Adolescents' online privacy: toward a developmental perspective, in: S. Trepte / L. Reinecke (eds.), Privacy online, 221-234. Heidelberg: Springer.

Prenksy, M. (2001), Digital Natives, Digital Immigrants, 9 On the Horizon 1.

Preston, C.B. / Crowther, B. T. (2014), Legal Osmosis: The Role of Brain Science in Protecting Adolescents, 43(2) Hofstra Law Review 447.

Rooney T. / Taylor E. (2017) (eds.), Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People, Routledge.

Rozendaal, E. / Buijzen M. / Valkenburg P. (2010), Comparing Children's and Adults' Cognitive Advertising Competences in the Netherlands, 4 (1) Journal of Children and Media 77.

Rozendaal, E. / Lapierre, M. A. / van Reijmersdal, E. A. / Buijzen, M. (2011), Reconsidering advertising literacy as a defense against advertising effects, 14 (4) Media Psychology, 338.

Savin-Williams, R. C. / Berndt, T. J. (1990), Friendship and peer relations, in: S.S. Feldman & G. Elliot (eds.), At the threshold: The developing adolescent, 277-307. Cambridge, MA: Harvard University Press.

Savirimuthu, J. (2016), Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests?, in: I. Iusmen / H. Stalford (eds.), The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions, 221-257, Barbara Budrich Publishers.

Schaub, F. / Balebako, R. / Durity, A.L. / Cranor, L. F. (2015), A Design Space for Effective Privacy Notices, 11th Symposium on Usable Privacy and Security (SOUPS 2015), https://www.usenix.org/system/files/conference/soups2015/soups15-paper-schaub.pdf

Sibony, A.-L. / Helleringer, G. (2015), EU Consumer Protection and Behavioral Sciences: Revolution or Reform?, in: A.-L. Sibony / A. Alemano (eds.), Nudge and the Law: A European Perspective, 209-233, Hart Publishing.

Steeves V. (2014b), Young Canadians in a Wired World, Phase III: Online Privacy, Online Publicity. Ottawa: MediaSmarts.

Steeves, V. (2014a), Young Canadians in a Wired World, Phase III: Life Online, MediaSmarts

Steeves, V. (2017), Terra Cognita: The Surveillance of Young Peoples' Favourite Websites, in: T. Rooney / E. Taylor (eds.), Surveillance Futures: Social and Ethical Implications of New Technologies for Children and Young People, 174-187, Routledge.

Steijn, W. (2014), Developing a sense of privacy, Phd dissertation, available at: https://pure.uvt.nl/ws/files/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf.

Steijn, W.M.P. / Schouten, A.P. (2013), Information sharing and relationships on social network sites. Cyberpsychology, Behavior, & Social Networking, 16(8), 582-587.

Steinberg, L. (2007), Risk taking in adolescence: New perspectives from brain and behavioral science, 16 Current Directions in Psychological Science 55.

Steinberg, L. (2008), A social neuroscience perspective on adolescent risk-taking, 28 Developmental Review 78.

Stuyck, J. / Terryn, E. / van Dyck, T. (2006), Confidence through fairness? The new directive on unfair business-to-consumer commercial practices in the internal market, 43 Common Market Law Review 107.

Subrahmanyam, K. (2008), Communicating online: Adolescent relationships and the media, The Future of Children, 18 Children and Media Technology 119.

Subrahmanyam, K. / Garcia, E.C.M. / Harsono, L.S. / Li, J. S. / Lipina, L. (2009), In their worlds: Connecting online weblogs to developmental processes, 27 British Journal of Developmental Psychology 219.

Sunstein, C.R. (2014), Nudging: A Very Short Guide, 37 Journal of Consumer Policy 583.

Svantesson, D. J. B. (2017), Enter the quagmire – the complicated relationship between data protection law and consumer protection law, Computer Law & Security Review, in press, doi: 10.1016/j.clsr.2017.08.003.

Tapscott, D. (1998), Growing up digital: the rise of the Net generation, McGraw-Hill.

Thaichon, P. (2017), Consumer socialization process: The role of age in children's online shopping behavior, 34 Journal of Retailing and Consumer Services 38.

Third, A. / Bellerose, D. / Dawkins, U. / Keltie, E. / Pihl, K. (2014), Children's Rights in the Digital Age: A Download from Children Around the World, Young and Well Cooperative Research Centre, Melbourne.

UK Children's Commissioner (2017), Growing up Digital: A Report of the Growing Up Digital Taskforce, January 2017.

Valant, J. (2015), Consumer protection in the EU Policy overview, September 2015, available at: http://www.europarl.europa.eu/ReData/etudes/IDAN/2015/565904/EPRS_IDA(2015)565904_EN.pdf

Valkenburg, P.M. / Peter, J. (2008), Adolescents' identity experiments on the internet: consequences for social competence and self-concept unity, 35(8) Communication Research 208.

Van der Hof, S. (2016), I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World, 34 Wis. Int'l L.J. 409.

Van der Hof, S. / Prins C. (2008), Personalisation and its Influence on Identities, Behaviour and Social Values, in: Hildebrandt M. / Gutwirth S. (eds) Profiling the European Citizen: Cross–disciplinary perspectives, 111-117, Springer, Dordrecht.

Verdoodt, V. / Clifford, D. / Lievens, E. (2016), Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU, 32 Computer Law & Security Review 599.

Waddington, L. (2014), Reflections on the Protection of 'Vulnerable' Consumers under EU Law, Maastricht Faculty of Law Working Paper No. 2013-2.

Waterman, A.S. (1982), Identity development from adolescence to adulthood: an extension of theory and a review of research. 18 (3) Developmental Psychology 341.

Wauters, E. / Lievens, E. / Valcke, P. (2013), A legal analysis of Terms of Use of Social Networking Sites, including a practical legal guide for users: 'Rights & obligations in a social media environment' (EMSOC - User Empowerment in a Social Media Culture No. D1.2.4), Leuven: iMinds-ICRI.

Wauters, E. / Lievens, E. / Valcke, P. (2015), Children as social network actors: A European legal perspective on challenges concerning membership, rights, conduct and liability, 31 Computer Law & Security Review 351.

Weitzenböck, E. M. (2014), Crowdsourcing and user empowerment: a contradiction in terms?, in: A. Savin / J. Trzaskowski (eds.), Research Handbook on EU Internet Law, 461-487, Edward Elgar Publishing Limited.

Wong, R. / Savirimuthu, J. (2008), All or nothing: this is the question? The application of Art. 3(2) data protection directive 95/46/EC to the internet, 25(2) The John Marshall Journal of Information Technology and Privacy Law 241.

Wu, H.-A. (2016), Video Game Prosumers: Case Study of a Minecraft Affinity Space, 42 Visual Arts Research 22.

Xanthoulis N. (2014) Negotiating the EU Data Protection Reform: Reflections on the Household Exemption, in: Sideridis A. / Kardasiadou Z. / Yialouris C. / Zorkadis V. (eds.) E-Democracy, Security, Privacy and Trust in a Digital World, 135-153, Springer, Cham.

Additional Sources

Article 29 Working Party, Opinion 10/2004 on more harmonised information provisions. 11987/04/EN, WP 100, November 2004.

Article 29 Data Protection Working Party, Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools), WP 160, 11 February 2009.

Article 29 Data Protection Working Party, Opinion 5/2009 on Online Social Networking, WP 163, 12 June 2009.

Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioral advertising, WP 171, 22 June 2010.

Article 29 Data Protection Working Party, Opinion 02/2013 on Apps on Smart Devices, WP 202, 27 February 2013.

Article 29 Data Protection Working Party, Statement of the Working Party on current discussions regarding the data protection reform package - Annex 2 Proposals for Amendments regarding exemption for personal or household activities, 27 February 2013.

Consumer Protection Cooperation Network (2013), Common position of national authorities within the CPC on online games, available at: http://ec.europa.eu/consumers/enforcement/cross-border_enforcement_cooperation/docs/common_position_on_online_games_en.pdf

Consumer Protection Cooperation Network (2017), Common position of national authorities within the CPC Network concerning the protection of consumers on social networks, available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=55999

Belgian Privacy Commission (2002), Advice No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet, available at: https://www.privacycommission.be/sites/privacycommission/files/documents/advies_38_2002_0.pdf (Dutch); https://www.privacycommission.be/sites/privacycommission/files/documents/avis_38_2002_0.pdf (French)

EDPS (2012), Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", 17 July 2012.

EDPS (2014), Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy, 14 March 2014.

EDPS (2017), Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content, 14 March 2017.

Electronic Privacy Information Center (2012), In Short: Advertising and Privacy Disclosures in a Digital World, available at: https://epic.org/privacy/ftc/FTC-In-Short-Cmts-7-11-12-FINAL.pdf

European Commission, Commission Staff Working Document, Guidance on the Implementation/Application of Directive 2005/29/EC on Unfair Commercial Practices, 25 May 2016, SWD(2016) 163 final.

European Commission, Consumer vulnerability across key markets in the European Union, Final report, January 2016, available at: http://ec.europa.eu/consumers/consumer_evidence/market_studies/docs/vulnerable_consumers_approved_27_01_2016_en.pdf

European Commission, DG JUSTICE Guidance Document concerning Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive

85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 13 June 2014, available at: http://ec.europa.eu/justice/consumer-marketing/files/crd_guidance_en.pdf

European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behavior, March 2016, available at: http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/final_report_impact_marketing_children_final_version_approved_en.pdf

European Commission (2014), Commission and Member States to raise consumer concerns with app industry, Press Release, 27 February 2014, available at: http://europa.eu/rapid/press-release_IP-14-187_en.htm

European Consumer Consultative Group (2013), Opinion on Consumers and Vulnerability, 7 February 2013, available at: http://ec.europa.eu/consumers/empowerment/docs/eccg_opinion_consumers_vulnerability_022013_en.pdf.

European Parliament, Report on a strategy for strengthening the rights of vulnerable consumers, 8 May 2012 (2011/2272(INI)), available at: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2012-0155&language=EN

European Parliament, Legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), P7_TA(2014)0212.

Eurostat (2016) E-commerce statistics for individuals, available at: http://ec.europa.eu/eurostat/statistics-explained/index.php/E-commerce_statistics_for_individuals#Proportion_of_e-shoppers_growing_steadily.2C_with_the_biggest_increase_among_young_people

Finnish competition and Consumer Authority (2015), Facts and Advice: A child needs a parent's consent to make purchases, available at: http://www.kkv.fi/en/facts-and-advice/buying-and-selling/children-as-consumers/children-as-shoppers/

ICO, The Guide to Data Protection, 11 May 2016, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-4.pdf

International Conference of Data Protection and Privacy Commissioners (2009), International Standards on the Protection of Privacy with regard to the processing of Personal Data (the Madrid Resolution), 5 November 2009.

OFCOM (2016), Children and parents: media use and attitudes report, available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf.

Office of Fair Trading (2014), The OFT's Principles for online and app-based games, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf

UK Advertising Standard Authority (2010), UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing, edition 12.

UN Committee on the Rights of the Child, General Comment No. 12: The Right of the Child to be Heard, UN Doc. CRC/C/GC/12, 20 July 2009.

Chapter 5

The "riskification" of European data protection law through a two-fold shift

Published in a peer-reviewed journal as:

Macenaite M., The "riskification" of European data protection law through a two-fold shift the European Journal of Risk Regulation, 8(3) 2017, pp. 506-540

Abstract

The importance of the concept of risk and risk management in the data protection field has explosively grown with the adoption of the General Data Protection Regulation (2016/679). The article explores the concept and the role of risk, as well as associated risk regulation mechanisms in EU data protection law. It shows that with the adoption of the General Data Protection Regulation there is evidence of a two-fold shift: first on a practical level, a shift towards risk-based data protection enforcement and compliance, and second a shift towards risk regulation on the broader regulatory level. The article analyses each of these shifts to enhance the understanding of the changing relationship between risk and EU data protection law. The article also discuses associated potential challenges when trying to manage multiple and heterogeneous risks to the rights and freedoms of individuals resulting from the processing of personal data.

Keywords: General Data Protection Regulation, Directive 95/46/EC, risk, risk-based approach, risk regulation.

I. Introduction

Personal data is becoming the driver and the most valuable commercial asset for many current business models both online and offline. Technological advancements, such as those related to big data applications or Internet-connected devices, rely increasingly on capturing and processing of personal data on a large scale. In parallel, based on the analysis of the collected data, individual decision-making may be enabled or influenced. Smart, data-generating devices create new complex risks, which differ from the traditional safety risks (i.e. to consumers and the environment) stemming from the more common industrial products.[562] Indeed, as noted by Spina, "the additional smart feature modifies the risk profile of the use of the product" [563]. The author goes on to further observe that personal data-driven products and services demand a different trade-off between the risks and alleged benefits and thus raise complex challenges in the accounting for ethical issues when assessing and managing risks.[564] Although the development of the data-driven economy is desirable for the EU Digital Single Market and the many benefits it affords individuals, this development cannot come at the

[562] A. Spina (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. European Journal of Risk Regulation, 8(1), 88-94.
[563] Ibid., 92.
[564] Ibid.

expense of fundamental rights and freedoms. In trying to balance these two (in essence contradictory) goals, the EU is repeatedly delineating the right to data protection, established in Article 8 of the Charter of Fundamental Rights of the European Union, as a qualified right, which needs to be balanced with other competing fundamental rights and interests, such as the freedom to conduct a business.[565]

The EU has recently reformed its regulatory framework, adopting the General Data Protection Regulation (2016/679)[566] (hereinafter – 'GDPR' or 'Regulation') which will come into force on the 25th of May 2018 and will replace the Data Protection Directive (Directive 95/46/EC)[567]. In trying to satisfy the same two goals as its predecessor namely, to ensure the functioning of the internal market through free personal data flows and to safeguard the fundamental right to privacy and personal data protection of the data subjects,[568] the GDPR relies heavily on risk and builds a substantial number of the new provisions around it. In essence, risk has become a new boundary in the data protection field and a key indicator in deciding whether additional legal and procedural safeguards are required in a particular context in order to shield data subjects from potential negative impacts stemming from specific data processing activities. In this vein Spina notes, that EU data protection legislation is undergoing a progressive"*riskification*".[569] He defines the 'riskification' as a shift 'from the limited boundaries of formal legality of processing of data and enforcement of individual rights against companies' towards 'a model of "enforced self-regulation" for managing technological innovation in uncertain scenarios'[570]. This model entails different governance measures that data controllers should rely on when controlling risks, such as data protection impact

[565] Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* (2010) ECR I-0000. See also Recital 4 of the General Data Protection Regulation which states: "*The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity*." Article 29 Working Party: *"The protection of personal data is a fundamental right. Personal data (which includes metadata) may not be treated solely as an object of trade, an economic asset or a common good" and "Data protection rights must be balanced with other fundamental rights, including non-discrimination and freedom of expression, which are of equal value in a democratic society." Joint Statement of the European Data Protection Authorities assembled in the Article 29 Working Party, WP 227 (2014), 26 November 2014,* 2.

[566] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[567] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (1995) OJ L281/31.

[568] The General Data Protection Regulation, in addition to these two main goals, introduces several additional new goals, such as the accomplishment of an area of freedom, security and justice and an economic union, economic and social progress, the strengthening and the convergence of the economies within the internal market, and the well-being of natural persons (Recital 2).

[569] A. Spina (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. European Journal of Risk Regulation, 8(1), 88-94. The term 'riskification' has been borrowed for the title of this article from A. Spina (cited above), who was the first to use it in the data protection context. Yet, this term was first introduced in security studies and although used in a different policy domain can provide interesting insights for data protection, especially when thinking about information security risks. see Olaf Corry, Securitisation and 'Riskification': Second-order Security and the Politics of Climate Change, Millennium, Vol 40, Issue 2, pp. 235- 258 See also William Clapton, Risk in International Relations, International Relations, Vol 25, Issue 3, pp. 280 – 295.

[570] A. Spina (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. European Journal of Risk Regulation, 8(1), 89.

assessments, the appointment of data protection officers, and regulatory strategies to implement data protection by design and by default.[571]

Although since the start of the data protection reform, much has been written on the GDPR and its envisaged novelties, the changing relationship between risk and EU data protection law is still substantially unexplored. The debate around risk regulation and data governance is just nascent among regulation and governance scholars who are starting to examine connections between digital data, ethics and risks.[572] Some legal contributions have analysed the injection of the risk-based approach into data protection and its implications[573] or future related challenges[574], but few[575] have extensively looked into the multidimensional concept of risk and how it shapes the GDPR as a regulatory instrument. The main purpose of the article is to explore the concept and the role of risk, as well as associated risk regulation mechanisms in EU data protection law. It does so by categorizing data protection law as undergoing a two-fold shift: on the practical enforcement level though a shift towards risk-based data protection and, on the broader regulatory level, towards risk regulation. The article analyses each of these shifts to enhance the understanding of risk and associated challenges when trying to manage multiple and heterogeneous risks to the rights and freedoms of individuals resulting from the processing of personal data.

First, the article more generally explores the relationship between risk and regulation. It draws on the regulation and governance disciplines to conceptually distinguish between risk regulation and a risk-based approach to regulation (or risk-based regulation). Next, the first shift towards risk-based regulation illustrated through the increased reliance on the risk concept in the Data Protection Directive and the GDPR is analysed. Then, the second shift towards risk regulation is explored comparing the GDPR with other EU risk-regulation domains (in particular, based on the existing risk scoring and assessing systems, the institutional arrangements and public participation in risk regulation). Finally, the paper concludes by outlining some unresolved challenges stemming from the two shifts.

---

[571] A. Spina (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. European Journal of Risk Regulation, 8(1), 88-94.

[572] Part of the forward-looking research agenda delineated in the inaugural issue of the recent European Journal of Risk Regulation is dedicated to risk regulation, data protection and ethics. See A. Spina (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. European Journal of Risk Regulation, 8(1), 88-94.

[573] Raphaël Gellert, 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5(1) International Data Privacy Law, *3-19*. Raphaël Gellert, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection, European Data Protection Law Review, Volume 2 (2016), Issue 4, 481 – 492; Niels van Dijka, Raphaël Gellerta, Kjetil Rommetveitb, A risk to a right? Beyond data protection risk assessments, Computer Law & Security Review, 32 (2), 2016, 286–306.

[574] Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, and Orla Lynskey , Risk management in data protection, International Data Privacy Law, 2015 5 (2): 95-98.

[575] One of the few existing comprehensive efforts to address risk-based approach in the GDPR is Quelle, Claudia, The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too (July 11, 2017). R Leenes, R van Brakel, S Gutwirth and P De Hert (eds), Data Protection and Privacy: The Age of Intelligent Machines (Hart Publishing, Forthcoming); Tilburg Law School Research Paper No. 17, available at SSRN: https://ssrn.com/abstract=3000382. To a certain degree the notion of risk in the GDPR has been also recently analysed by István Böröcz, Risk to the Right to the Protection of Personal Data: An Analysis Through the Lenses of Hermagoras, European Data Protection Law Review, Volume 2 (2016), Issue 4, 467 – 480 (he distinguishes several basic attributes of risk to the right of personal data protection, such as the meaning of risk, subjects exposed to/conceptualising risk, the time and means to address risks)

II. Risk and Regulation

Risk regulation has initially developed in relation to the legal instruments and management techniques of environmental, human health and safety hazards. To address these hazards, regulators started setting up legal frameworks based on the tripartite management of intrinsic risks, i.e. risk assessment, risk management, risk communication.[576] Risk regulation, thus, has emerged as a model to control risks stemming from new technologies or industries and to address related market failures, such as information asymmetry or unwanted side-effects of the progressive advancements. During the last two decades, however, the role of risk has increasingly grown and diversified in various national and international regulatory regimes, private business settings and wider governance systems.[577] In parallel with risk regulation, risk-based regulation appeared, as a model relying on a proportionate and targeted strategy for regulatory enforcement primarily with the aim to manage the resources and reputation of regulators. This strategy has grown in popularity and risk for the regulators has increasingly become 'a new lens through which to view the world'[578]. In part as the result of the 'regulatory crisis' experienced by many European countries throughout the 1980s and 1990s, risk-based regulation represents an effort to fight against over-regulation, legalistic and prescriptive rules, and the high costs of regulation.[579] It has been argued that more evidence-based policy making, reliance on economic cost-benefit approaches, and the usage of scientific risk-assessment tools and techniques can lead to more objective, transparent and better cost-benefit balanced regulation.[580] As a result, this climate favored a conscious orientation towards risk-based regulation across many different policy domains ranging far beyond the environmental and human safety areas, such as finance, utility, housing, child protection.[581] Risk became a central concept not only in regulation, but also in broader governance terms, relating to a multitude of private and public actors, purposes and instruments and thus, 'a significant organizing principle of government' and 'a benchmark of good governance'.[582]

The expansion and diversity of risk functions in regulation and governance with time can be better grasped through three aspects of the relationship between risk and regulation. First, a growing amount of modern societal risks stemming from technological and scientific advancements appeared or have been discovered and required mitigation through regulation, i.e. societal risks directly pushed forward unmediated regulatory response, often beyond the limits of a single state.[583] Risk became an object for regulation and helped to justify regulatory

---

[576] See E.Fisher Risk Regulation and Administrative Constitutionalism 2007.

[577] Beck, U. (1992) Risk Society, London: Sage; Jasanoff S. (1999) 'The songlines of risk', Environmental Values 8: 135, 52. Hood C., Rothstein, H. and Baldwin, R. (2001) The Government of Risk: Understanding Risk Regulation Regimes, Oxford: Oxford University Press; Garland, D.(2003) 'The rise of risk', in R. Ericson and A. Doyle (eds) Risk and Morality, Toronto: University of Toronto Press; Smith, M. (2004) 'Mad cows and mad-money: problems of risk in the making and understanding of policy', The British Journal of Politics and International Relations 6(3). Michael Power, *The Risk Management of Everything—Rethinking the Politics of Uncertainty* (Demos, London 2004)

[578] Bridget M. Hutter, 'The Attractions of Risk-based Regulation: accounting for the emergence of risk ideas in regulation' (2005) Centre for Analysis of Risk and Regulation, Discussion paper No. 33, 1-21, 1, <http://grammatikhilfe.com/researchAndExpertise/units/CARR/pdf/DPs/Disspaper33.pdf>, accessed 4 November 2014, 1.

[579] Ibid., 1-3

[580] Ibid.

[581] Rothstein, Henry, Huber, Michael, Gaskell, George, A theory of risk colonization: the spiralling regulatory logics of societal and institutional risk, Economy and society, 35(1) 91-112, 2006

[582] Julia Black, 'The Role of risk in regulatory processes' in Robert Baldwin, Martin Cave, Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press, New York, 2010) 302-348, 303.

[583] Rothstein, Henry, Huber, Michael, Gaskell, George, A theory of risk colonization: the spiralling regulatory logics of societal and institutional risk, Economy and society, 35(1) 91-112, 2006

interventions.[584] As argued by Beck in his famous 'Risk Society', late modernity is characterised by the replacement of class relationships with risk relationships, which are key elements in societal conflict and change.[585] Power adds that in our current 'risk society' we are dealing with the 'risk management of everything'[586].

Second, on the institutional level, the scope and character of the regulatory frameworks changed. It has been argued that in the last half of the 20th century the 'regulatory state' emerged, i.e. the role of the state shifted from redistributive welfare to the improvement of economic efficiency and developing regulatory frameworks, institutions and mechanisms.[587] Independent regulatory agencies appeared, which could gather scientific evidence and strengthen the focus on risk. Enhanced scrutiny and control of regulatory behaviours also allowed for regulators to better define their regulatory goals, understand limited regulatory capacity and institutional risks related to their regulatory activities. Risk thus came in operationalizing the goals of regulators.[588] Third, risk also became 'a method for organising regulatory activity', for example it allowed for the prioritisation of regulatory enforcement or standard setting according to the seriousness of the related risks.[589] It defined organizational accountability and evaluation.[590] As summarized by Black in the context of public institutions, 'risk-based regulation involves the development of decision-making frameworks and procedures to prioritise regulatory activities and the deployment of resources, principally inspection and enforcement activities, organised around the assessment of the risks that regulated firms pose to the regulators objectives'[591].

The importance of risk to regulation and governance stems not only from the risk society and the growing amount of diverse societal risks but also from the frameworks themselves aiming to regulate these risks that are inherently entailing institutional risks. Some authors called this a simultaneous expansion of the duality of risks[592] and others emphasising the dynamic interaction between societal and institutional risks referred to 'the colonisation of regulatory decision-making by risk' and its spiralling aspect.[593]

2.1. Risk regulation in the EU

Risk regulation has been particularly visible across the policies of the European Union, albeit not equally, such in as environmental, agro/food and financial sectors. An increasing

[584] Julia Black, 'The Role of risk in regulatory processes' in Robert Baldwin, Martin Cave, Martin Lodge (eds), The Oxford Handbook of Regulation (Oxford University Press, New York, 2010) 302-348, 303.
[585] Beck, U.(1992) Risk Society, London: Sage.
[586] Michael Power, *The Risk Management of Everything—Rethinking the Politics of Uncertainty* (Demos, London 2004)
[587] Majone, G. (1994) The Rise of the Regulatory State in Europe. West European Politics, 17, 77-101. Loughlin, M. and Scott, C. 1997 'The Regulatory State', in P. Dunleavy, I. Holliday, A. Gamble and G. Peele (eds) Developments in British Politics 5, Basingstoke: Macmillan.
[588] Julia Black, 'The Role of risk in regulatory processes' in Robert Baldwin, Martin Cave, Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press, New York, 2010) 302-348, 303.
[589] Rothstein, Henry, Huber, Michael, Gaskell, George, A theory of risk colonization : the spiralling regulatory logics of societal and institutional risk, Economy and society, 35(1) 91-112, 2006, 97.
[590] Julia Black, 'The Role of risk in regulatory processes' in Robert Baldwin, Martin Cave, Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press, New York, 2010) 302-348, 303.
[591] Black, Julia (2005) *The emergence of risk-based regulation and the new public management in the United Kingdom.* Public Law, 2005, pp. 512-549, 514.
[592] Claudio Ciborra, Digital technologies and the duality of risk, CARR discussion paper No. 27, CARR LSE: London. http://eprints.lse.ac.uk/36069/1/Disspaper27.pdf Michael Power, *The Risk Management of Everything—Rethinking the Politics of Uncertainty* (Demos, London 2004) (Power argues that institutional risks are secondary risks in relation to the societal risks)
[593] Rothstein, Henry, Huber, Michael, Gaskell, George, A theory of risk colonization : the spiralling regulatory logics of societal and institutional risk, Economy and society, 35(1) 91-112, 2006 , p. 105.

number of regulatory activities have been framed in terms of risk with risk providing justification for regulation. Regulation of human health and safety in the EU, for example, is clearly defined in terms of risk. One of the policy aims in the EU food safety area is to prevent, eliminate or reduce to an acceptable level risks to humans and animals.[594] Thus, as noted by Alemanno, risks to human health and safety do not only constitute an object for regulation, but also 'one of the rationales for the EU regulatory action'.[595] Indeed, it is claimed that we could see an emerging European risk regulation model, even if in its embryonic stage, which not only uses the classical risk analysis framework (risk assessment, management, communication), but also has its own particular features, such as regulatory impact assessments, reliance on precautionary and proportionality principles, consideration of legitimate (non-scientific) factors in the risk management stage, and a general tension between the rational, evidence-based and flexible, precautionary decision-making.[596]

Although there is no uniform analytical approach to risk and scientific risk assessments in the EU are conducted by various EU bodies following different, often diverging, methodologies, a number of EU laws include risk assessment procedures. For example, the Regulation 178/2002 protecting human health and consumers' interest in relation to food, establishes the principle that food law is based on risk analysis, comprising three interconnected processes: risk assessment, risk management and risk communication.[597] In the same vein, risk assessment plays an important role in the area of chemicals and products. The Regulation on chemicals[598], the Plant Protection Regulation[599] and the Cosmetics Regulation[600] require the assessment of the risks of chemicals and products based on their specific hazardous properties and exposure to them in two steps: first, hazard identification and characterization (the potential to cause harm) and then risk assessment (the likelihood of harm). The extent to which in practice regulatory decisions rely on both steps (classification of hazards and assessment of risks), however, seems to be questionable.[601] The Medical product Directive[602] makes medical product authorization subject to a favorable risk-benefit balance and requires the setting up of a risk management systems, i.e. a set of activities designed to identify, characterise, prevent or minimise risks relating to a medicinal product.

---

[594] Regulation (EC) No 882/2004 of the European Parliament and of the Council of 29 April 2004 on official controls performed to ensure the verification of compliance with feed and food law, animal health and animal welfare rules (2004) OJ L 165, with later amendments by Regulation (EC) No 1029/2008 (2008) OJ L 278 and Regulation (EC) No 596/2009 (2009), OJ L 188.

[595] Alberto Alemanno, 'Regulating the European Risk Society', in Alberto Alemanno, Frank den Butter, André Nijsen and Jacopo Torriti (eds), *Better Business Regulation in a Risk Society* (Springer, New York 2013), 37-56.

[596] Alemanno (supra note).

[597] Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (2002) OJ L 31.

[598] Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) and establishing a European Chemicals Agency (2006) OJ L 396/1, as amended.

[599] Regulation (EC) No 1107/2009 of the European Parliament and of the Council of 21 October 2009 concerning the placing of plant protection products on the market and repealing Council Directives 79/117/EEC and 91/414/EEC (2009) OJ L 309/1

[600] Regulation (EC) No 1223/2009 of the European Parliament and of the Council of 30 November 2009 on cosmetic products (2009) OJ L 342/59.

[601] Kristina Nordlander, Carl-Michael Simon and Hazel Pearson, 'Hazard v. Risk in EU Chemicals Regulation' (2010) *European Journal of Risk Regulation 3,* 239-250, 240.

[602] Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (2001) OJ L 311/67

2.2. Risk-based approach to regulation

The essence of risk-based regulation is providing a model to achieve a proportionate and adaptive strategy for regulatory enforcement.[603] It allows the regulatory bodies to set priorities and explicitly explain their selective decisions based on the assessment of the risk that the regulated actors (companies or individuals) present.[604] Although risk-based regulatory models can vary depending on the policy domain, the particular country and in their complexity, they all start from the basic premise that it is impossible and costly to entirely eliminate all hazards and risks.[605] Therefore, the focus is on identifying the risks that the regulators want to manage instead of enforcing all the existing rules on all the regulated entities.[606]

Black and Baldwin distinguish five main features shared by the majority of the risk-based frameworks that can be summarised as follows.[607] First, the regulators that use these frameworks define their own objectives and the risks to their achievement. Second, regulators determine the acceptance threshold for specific risks and their level (risk appetite). Third, they assess risks that the regulated actors present in terms of negative impact and probability or likelihood. The terminology (in human safety the focus is on hazards and exposure while in financial sector on impact and probability) and methodology (qualitative or quantitative) differ depending on the policy area. Fourth, regulators use the assigned numerical scores or categories in order to rank and prioritise the actors, their activities or policy issues. Finally, they allocate resources for supervisions, inspection and enforcement based on the rankings mentioned above. As the regulators following a risk-based approach focus their regulatory activities and resources on the most risky and harmful policy outcomes, this allows them to solve their wider legitimacy and accountability problems. It is claimed, that reliance on risk and emphasis on rational decisions can help bureaucracies to justify their decisions in terms of technocratic legitimacy regardless of the real methodological value of such decisions.[608] Thus, risk-based frameworks may also be seen as techniques used by regulators 'to shift or dissipate blame'[609] or even to set forth when blame should fall on them in the first place.[610] Risks that are defined

---

[603] Some confusion exists between the terms of 'risk regulation', 'risk-based regulation' and 'risk-based approach to regulation' due to the conflating meanings these terms are assigned by various authors. Black, for example, in her work refers to risk-based regulation as having two distinct meanings: 1) the regulation of societal risks to health, safety, the environment and financial wellbeing. In this sense, risk-based regulation determines whether public institutions should regulate specific activity and which preventive measures employ; 2) refers to the risk that a public institution will not meet its objectives (regulatory or institutional risk) and denotes procedures and decisions to prioritize activities and resources based on risk assessment that regulated entities pose. Black, Julia (2005) The emergence of risk-based regulation and the new public management in the United Kingdom. Public Law, 2005, pp. 512-549, 514.

[604] Robert Baldwin, Martin Cave, Martin Lodge, *Understanding Regulation: Theory, Strategy and Practise* (2 ed., Oxford University Press, New York 2012) 281-282.

[605] Cass R. Sunstein, *Risk and reason: Safety, law, and the environment* (CUP Cambridge 2002); Robert Baldwin, Julia Black 'Really Responsive Risk-Based Regulation' (2010) 3 Law and Policy 2(2), 181-213; Julia Black, Robert Baldwin, 'When risk-based regulation aims low: Approaches and challenges' (2011) Regulation and Governance 6(1), 2-22. D John Graham J 'Why Governments Need Guidelines for Risk Assessment and Management' in OECD, *Risk and regulatory policy: Improving the governance of risk* (OECD, Paris 2010).

[606] Julia Black, Robert Baldwin 'Really Responsive Risk-Based Regulation' (2010) 3 Law and Policy 2(2), 184.

[607] Ibid., 184.

[608] Theodore M. Porter, Trust in Numbers: The Pursuit of Objectivity in Science and Public Life (Princeton, Princeton University Press 1995)

[609] Julia Black, 'The Role of risk in regulatory processes' in Robert Baldwin, Martin Cave, Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press, New York, 2010), 323. Also C. Hood 'The Risk Game and the Blame Game', 2002, *Government and Opposition*, 37:15-37.

[610] Julia Black, 'The Role of risk in regulatory processes' in Robert Baldwin, Martin Cave, Martin Lodge (eds), *The Oxford Handbook of Regulation* (Oxford University Press, New York, 2010), 323.

as tolerable by regulators, are thus considered to be politically acceptable, should not be expected to result in blame, once they occur.[611] In the rapidly changing and technologically complex environment such a defensive stance based on risk is ever more important for regulators of new technologies, as they are inevitably lagging behind in terms of intervention.

In practice, in the UK, an EU-member state that paved the way for European developments in risk-based approach to regulation, since 2005 risk has been shaping policies far beyond human health and safety or the environmental protection, i.e. the areas that are traditionally associated with risk. Risk also has been defining a wide range of policy processes, like information gathering, policy making, service delivery, implementation and enforcement. UK public administration has endorsed the risk-based approach and has been trying to achieve effective inspection and enforcement using risk-assessments to determine enforcement actions.[612] Public institutions are required to base their regulatory activities on risk when determining priorities in their area of competence and the allocating scarce resources. They are also expected to take into account risk at every stage of their decision-making processes, such as in selecting the most appropriate type of intervention, performing checks on compliance, and the taking of enforcement actions.[613]

The risk-based approach to regulation has had much more limited application in other Member States, where risk was incorporated into regulation principally because of international and EU constraints.[614] In France and Germany, for example, risk is still mainly used in policy domains traditionally concerned with risk, such as nuclear or food safety, the environment, or financial services. Risk in these Member States has also a more restricted role in framing regulatory processes, mainly only as far as such processes relate to obligatory risk assessments.[615]

2.3. Aligning risk-based regulation literature with data protection

Risk-based regulation literature discussed above deals with risk-based regulation as a regulatory strategy used by the governments and regulatory agencies to deal with societal and institutional risks in a risk-based manner. However, the GDPR in comparison, mainly relies on private entities, the data controllers, and to a large extent entrusts them with a detailed definition, assessment and management of societal risks related to their data processing activities. Nonetheless, the two at first sight diverging theoretical and practical perspectives on risk-based regulation can be aligned. On the one hand, as stated by Quelle, "under a decentred understanding of regulation, it is possible to see controllers themselves as regulators engaged in risk-based regulation as well as risk regulation"[616]. On the other hand, a regulator in the GDPR has arguably already prioritised some risks by establishing general criteria of high risk data processing operations and subjecting risky or highly risky processing operations to specific requirements, such as a representative in the EU, notification of supervisory authorities and data subjects about a data breach, maintenance of records, data protection impact

[611] Ibid.

[612] See Philip Hampton, 'Reducing Administrative Burdens: Effective Inspection and Enforcement' (Report) (March 2005) <http://webarchive.nationalarchives.gov.uk/+/http:/www.bis.gov.uk/policies/better-regulation/improving-regulatory-delivery/assessing-our-regulatory-system> accessed 12 February 2015.

[613] UK Department for Business Innovation and Skills, 'Better Regulation Delivery Office, Regulators' Code', (in particular, Principle 3 'Regulators should base their regulatory activities on risk') (April 2014) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/300126/14-705-regulators-code.pdf> accessed 12 February 2015.

[614] Henry Rothstein, Olivier Borraz, Michael Huber, 'Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe' (2013) *Regulation & Governance* 7, 215–235.

[615] Ibid.

[616] Claudia Quelle, The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too, 2017.

assessments and the prior consultation. Regulatory agencies, the national data protection authorities, can provide guidelines on impact assessments and further select and define risks to be prioritised and assessed by deciding on the detailed list of the processing presenting high risks. A part of the risk regulatory process, the actual risk assessment, a task which costs considerable time and effort, is 'outsourced' to data controllers.[617] In practice, however, this outsourcing raises serious fears: data protection authorities become a secondary and weaker players while the scope and the necessity of the private impact assessments is uncertain.[618] In addition, if the impact assessment reveals that data processing can result in high risk that the taken measures cannot mitigate, data controllers need to turn to data protection authorities for a prior consultation. This GDPR requirement follows a reversed logic than the general notification obligation present in its predecessor, as "the idea appears to be that, rather than sifting through endless notifications, supervisory authorities can sit back and wait until controllers start a prior consultation (…) on their own accord".[619] As a consequence, the GDPR risk-based provisions even if imposed directly on the data controllers as an end results allows the supervisory authorities to enforce the GDPR compliance in a risk-based manner, save resources and prioritise their enforcement activities.

III. The First Shift – Risk-Based Approach to Data Protection

3.1. The Emergence of the Idea

The idea to protect individuals based on potential risk and negative impact instead of considering all personal data inherently worthy of protection has emerged in the EU prior the launch of the data protection reform. It can be traced back to the RAND Europe Review of the Data Protection Directive, a key report in the data protection reform process, commissioned by the UK Information Commissioner's Office (ICO) in 2009.[620] The report underlined a missing clear link between the concept of personal data and real privacy risks, showing that not all data processing acts covered by the Directive 95/46/EC have a noticeable privacy impact on individuals.[621, 622] To create more effective protection in the future that focuses on the exchange and use of large amounts of personal data globally, the report suggested to look into the impact on privacy as a relevant criterion to determine the applicability of the data protection rules. In this sense, the RAND proposal is closer to a harm-based rather than a risk-based approach, which concentrates on the regulatory outcome (damage prevention) and does not extend to the

[617] Claudia Quelle, 'The data protection impact assessment: what can it contribute to data protection?' (LLM thesis, Tilburg University 2015) http://arno.uvt.nl/show.cgi?fid=139503, 112, 127.

[618] ME Gonçalves, The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward (2017) 26(2) *Information & Communications Technology Law* 90, 114.

[619] Claudia Quelle, The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too, 2017.

[620] N Robinson, H Graux, M Botterman and L Valeri, 'Review of the European Data Protection Directive' (The RAND Corporation technical report series 2009) www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf, 48-49, 51.

[621] Ibid., p. 27.

[622] Support for the risk-based approach has been expressed also in the responses to the Public consultations. See e.g. the Information Commissioner (United Kingdom), 'Response to "A comprehensive approach on personal data protection in the European Union A Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions"' (2010) <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf> accessed 5 February 2015 (the UK, already leading in risk-based regulation, has expressed its support for a GDPR as risk-based framework suggesting to focus obligations for data controllers on processing that poses genuine risk to individuals or society; to base the distinction between sensitive and ordinary data on the risk that particular processing poses to individuals in particular circumstances; to prioritise the areas of particular privacy risk as regards enforcement)

potential and actual adverse impacts.[623] Procedurally, the limited regulatory outcome of damage prevention is to be achieved largely by the data controllers themselves rather than through the ex ante process and obligations established by the regulatory framework. The GDPR did not take the harm-based approach, but if it had, risk analysis and management carried out by data controllers at their own discretion would dominate in the legal framework.[624]

Unsurprisingly, the idea of risk-based data protection has increasingly found support among different stakeholders. First, reliance on risk envisioned more effective and contextualised data protection instead of merely a compliance-based prescriptive framework. In other words, risk would enable to shift data protection from a box ticking exercise to protection on the ground by nuancing obligations for data controllers according to the risk involved. Kuner denotes the new obligation to evaluate risks using Data protection Impact Assessments as a part of a shift from 'paper-based bureaucratic requirements' towards 'compliance in practice'.[625] Second, the risk-based approach can be expected to enhance accountability, transparency and foster the data protection culture among data controllers. The European Commission perceives the evaluation of risks through the Data Protection Impact Assessments as a way to force the data controllers to assume more responsibility *vis-à-vis* data subjects.[626] The approach could even steer the data controllers "towards the least risky processing possible if this is rewarded by fewer and more appropriate obligations (scaled and proportionate to the risk involved)".[627] One more benefit of this approach is the flexibility as regards the future technological advancements. The risk based approach may provide a solution to the current data protection practises such as big data analytics or Internet of Things where the traditional compliance based approach does not work.[628] Application of the core principles, such as purpose limitation (purpose specification and compatible data use) and data minimisation, or reliance on the data subject's consent has become increasingly difficult when dealing with big data.[629] Finally, the turn to a more flexible risk-based legislation has been driven by economic argumentation - the internal market can be enhanced through reduction of administrative and compliance costs for companies. The discontent of the industry representatives with high financial and administrative burdens that data protection compliance causes and little actual protection for individuals brought by such formal compliance featured in responses to the European Commission's public consultations.[630]

---

[623] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', WP 218, 30 May 2014, p. 4.

[624] Claudia Quelle, The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too, 2017.

[625] Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) 11 Privacy & Security Law Report, 6, p. 1.

[626] Vivian Reding, 'Towards a true Single Market of data protection' (Speech at the Meeting of the Art. 29 Working Party 'Review of the Data protection legal framework', SPEECH/10/386, 14 July 2010) <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/386> accessed 14 February 2015.

[627] Digitaleurope, Comments on the risk-based approach, 28 august, 2013, available at: http://teknologiateollisuus.fi/sites/default/files/file_attachments/elinkeinopolitiikka_digitalisaatio_tietosuoja_digitaleurope_risk_based_approach.pdf

[628] Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?', 3 International Data Privacy Law (2013), p. 74. Mireille Hildebrandt, 'Slaves to Big Data. Or Are we?', October 2013, at 7, available at http://works.bepress.com/mireille_hildebrandt/52; Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics', 11 Northwestern Journal of Technology and Intellectual Property 239 (2013), at 252, to be found at SSRN: http://ssrn.com/abstract=2149364, p. 242 and 259.

[629] Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, The challenge of 'big data' for data protection, *International Data Privacy Law (2012) 2 (2)*

[630] European Commission, 'Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data' (2010) <http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf> accessed 5 February

The rhetoric of 'regulatory burdens', in particular for micro, small and medium-sized enterprises (SMEs) is not something completely new in the European regulatory arena. It has shaped a number of other legislative acts across various EU policy areas. Several different tactics have been used to shield the SMEs from regulatory burdens, such as exemptions from legal obligations, reduced record keeping duties, simplified inspection procedures, and obligations proportionate to risk, being just some of them.[631] For example, SMEs with fewer than 250 employees are not obliged to follow the neutral selection requirements in relation to women on company boards[632] or micro non-toxic pesticide distributors by national derogations can be exempted from the provisions of the Directive 2009/128/EC[633]. An example of the implemented risk-based approach, are Regulations 852/2004 and 853/2004 that require food producers to implement hygiene procedures based on risk and take measures in relation to identifiable hazards. As a result, the main underlying idea, at least of the Commission, has been to foresee lighter touch regulation to small-scale low risk data processing operations and, where possible, to lower the administrative and compliance burden for companies processing 'ordinary' personal data in today's information society. Similar examples of this so-called 'risk-burden balance model' can be found in several countries outside the EU, such as Japan and Australia, which exempt entities that are considered as presenting no danger for individuals (e.g. small entities, holders of limited amount of personal data for short time period) from data protection regulation activities.[634]

Being new and still emerging in its meaning, the risk-based approach has been advocated by various stakeholders in distinct interpretations. The narrowest interpretation, the most closely reflected in the adopted GDPR text, views risk as a yardstick to tailor data controllers' obligations.[635] In this sense, the risk-based approach means 'a scalable and proportionate approach to compliance'[636]. A broader version of the risk-based approach promulgated risk as an organizing concept not only for compliance but also for data protection enforcement. In this respect policing and enforcement carried out by data protection authorities should target risky rather than all data processing activities.[637] Those following the broadest

---

2015. Summary of the Replies to the Public Consultation on the Commission's Communication on a Comprehensive Approach on Personal Data Protection in the European Union (Annex 4) (2012) <http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf> accessed 5 February 2015

631 Cf. Adapting Legislation to Minimise Regulatory Burdens for SMEs: Best Practise Examples, Group of High Level National Regulatory Experts - SME Working Group (2013) <http://ec.europa.eu/smart-regulation/impact/best_practices_examples/docs/eu/lighter_regimes_for_smes_oct_2013.pdf> accessed 5 February 2015

632 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on improving the gender balance among non-executive directors of companies listed on stock exchanges and related measures' COM(2012) 614 final, 14 November 2012.

633 Directive 2009/128/EC of 21 October 2009 establishing a framework for Community action to achieve the sustainable use of pesticides, 24.11.2009, L 309/71.

634 Terwangne, Is a Global Data Protection Regulatory Model Possible, in Serge Gutwirth et. al. (eds.), Reinventing Data Protection?, Springer 2009, p. 180

635 Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", 14.1.2011, *("The higher the risks, the higher the need to implement concrete measures that protect information at a practical level and deliver effective protection"*, 21. EDPS claims that data protection law should be scalable, excluding the requirements of privacy by design, data protection officers and privacy impact assessments which should remain mandatory, p. 22-23).

636 Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', WP 218, 30 May 2014.

637 The Information Commissioner (United Kingdom), 'Response to "A comprehensive approach on personal data protection in the European Union A Communication from the European Commission to the European

interpretation have viewed the risk-based approach as eliminating core data protection principles or even data subjects' rights.[638] For example, industry representatives DigitalEurope proposed to keep data controllers responsible only for materialized privacy harms caused by the data processing and fully allow them to choose means to assess and mitigate the risks. As the regulatory outcome dominates over the process, according to the proposal, regulation and detailed rules on procedures and obligations for privacy harm prevention are burdensome and unnecessary.[639] The DigitalEurope proposal in essence aligns with the APEC Privacy Framework and its controversial primary principle to prevent harm to individuals[640], which considerably lowers the European data protection standards.

3.2. Risk and risk-based approach in the Directive 95/46/EC and the GDPR

Although the risk-based approach has been the subject of intense interest in the past years, in essence, reliance on risk as a concept cannot be considered a novelty in the area of personal data protection.[641] Indeed, the Data Protection Directive of 1995 referred to risk in five articles long before the term 'risk-based approach' entered the parlance of the EU policy makers during the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation.[642] Also, many national data protection laws already foresaw risk management as an explicit requirement.[643] Although the concept of risk does not entail radical changes, the functional role assigned to risk in the GDPR is novel compared to its predecessor. Starting with an overview of the roots of risk in the Directive 95/46/EC, the new functions of the risk concept in the GDPR are discussed below.

3.2.1. Root of the genesis of risk – data and information security

Risk has long been an essential integral component of data and information security. Already the early methodologies, that started emerging in 1990s in Europe, used risk assessment and management frameworks to protect networks and information assets from the threats to which they were exposed.[644] For example, the first national data security risk

---

Parliament, the Council, the Economic and Social Committee and the Committee of the Regions"' (2010), 8, <http://ec.europa.eu/justice/news/consulting_public/0006/contributions/public_authorities/ico_infocommoffice_en.pdf> accessed 5 February 2015

638 DigitalEurope, comments on the risk-based approach, 28 August 2013, 3. See also similar academic interpretations: Raphaël Gellert, We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection, European Data Protection Law Review, Volume 2 (2016), Issue 4, 481 – 492; Moerel, Lokke and Prins, Corien, Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things (May 25, 2016). Available at SSRN: https://ssrn.com/abstract=2784123 (Prins and Moerel suggest to focus more on the data use but do not exclude data collection from legal safeguards)

639 DigitalEurope, comments on the risk-based approach, 28 August 2013.

640 Asia-Pacific Economic Cooperation (APEC), Privacy Framework, 2005, available at: https://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx

641 Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN, WP218 (2014), 2.

642 The reference to risk in terms of breaching the privacy of data subjects is also present in 3 Recitals of the Data Protection Directive, namely: Recital 46 in the context of security measures, Recitals 53-54 in the context of notification and prior checking procedures.

643 Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, and Orla Lynskey , Risk management in data protection, International Data Privacy Law, 2015 5 (2): 95-98.

644 For a comprehensive overview of national risk management and assessment methodologies see ENISA Inventory of risks assessment and risk management methods, 30 March 2006, at:

assessment methodologies adopted by public institutions, such as the Dutch A&K analysis[645] developed in the 1980s, the British CRAMM methodology of 1985[646], the French MARION methodology of 1990[647] or the German IT- Grundschutz model of 1994,[648] provided a set of steps for IT security management through threat identification, characterization, exposure assessment and risk characterization. In the same vein, later developed international standards and tools,[649] such as ISO/IEC 27005:2011 on Information security risk management[650], provided frameworks for organizations to assess their information security risks based on a risk management approach.

The need to rely on risk in the information security field might be related to the shift from computer to information and data security.[651] While initially the information security concerns mainly lay with the physical site security, growing integration of various IT applications and systems and social and organisational components has led to increased complexity, incomplete human knowledge and uncertainty (e.g. unintended side effects caused by human intervention), which resulted in enhanced risks.[652] In addition, threats to information security have become increasingly global, sophisticated and continuously evolving, while (personal) data have grown into a valuable company asset.[653] Thus, there was a need and urgency "to take a holistic view of the risks associated with information systems and look at the threats arising from physical events, human failings as well as technological vulnerabilities and deliberate attacks"[654]. As a result, companies started integrating security risk management into the logic of mainstream management and business engineering in order to mitigate as much as possible the uncertainties and risks related to their information systems with limited resources. They turned to the toolsets and methodologies that were used in other management areas, such as financial risk management. Reliance on risk management methodologies essentially allowed them "to substitute(s) the unachievable and immeasurable goal of fully securing the information system with the achievable and measureable goal of reducing the risk that the information system faces to within acceptable limits".[655]

The aim of information and data security is to protect three main characteristics of information (data), which is oftentimes the primary asset of the company: confidentiality,

---

https://www.enisa.europa.eu/publications/inventory-of-risk-assessment-and-risk-management-methods. For a global overview of standards development see Jeffrey R. Yost, "History of Computer Security Standards." In Karl de Leuuw, ed., *History of Information Security* (Amsterdam: Elsevier Science, 2007): 595-621

645 Afhankelijkheids- en Kwetsbaarheidsanalyse (A&K analysis), RCC and Dutch ministry of internal affairs. Handbook: 'Handleiding Afhankelijkheids- en Kwetsbaarheidsanalyse: stappenplan voor de uitvoering van een A&K-analyse' (in Dutch), version 1.01, Ministry of Internal Affairs, The Hague, 1996, The Netherlands

646 CCTA Risk Analysis and Management Method, Central Communication and Telecommunication Agency,

647 Methodology of Analysis of Computer Risks directed by Levels, Club de la sécurité de l'information français, 1990

648 IT Baseline Protection Manual, Federal Office for Information Security, 1994.

649 See also OECD Guidelines for the security of Information Systems and Networks of 25 July 2002

650 ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management

651 The early sources focus on computer rather than information security, e.g. Donn B. Parker, Fighting Computer Crime: A New Framework for Protecting Information (New York: John Wiley & Sons, Inc., 1998). Deborah Russell and G. T. Gangemi, Sr., Computer Security Basics (New York: Thunder Mountain Press, 1994).

652 Ole Hanseth, Introduction: integration-complexity-risk-the making of information systems out of control, in Hanseth, Claudio Ciborra (eds.) Risk, Complexity and ICT, 2007

653 Alan Calder, Steve Watkins, IT Governance: An International Guide to Data Security and ISO27001/ISO27002, 6th ed., 2015.

654 Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security, *OJ C 48, 28.2.2003, p. 1–2*

655 John Vacca, Computer and Information Security Handbook, 2nd Edition, 2013, p. 906.

integrity, availability[656], the commonly called CIA triad. This triad reveals the goal to ensure that information does not become available to unauthorized individuals, entities or processes, that it remains accurate and complete, and that information (and its supporting assets) can be accessed and used when needed by the authorized individuals and entities.

The field of information and data security has its own aim, predefined (yet continually evolving) vocabulary and thus its own interpretation of risk. Risk, essentially refers to the probability that a vulnerability of an asset (intentionally or non-intentionally) is exploited by a threat and negatively affects the three above mentioned characteristic of information (data) and the impact of that effect.[657] According to Vacca, risk might be expressed as the following function of four elements R= f(A,T,V,I), where: (a) A, the value of the assets; (b) T, the severity and likelihood of the threat; (c) V, the nature and the extent of vulnerabilities and the likelihood that a threat can successfully exploit them; d) I, the likely impact of the harm, if the threat occurs.[658]

As evidenced by the above definition, the components of risk, revolve around several main subjects that also constitute not only specific vocabulary of information security experts, but also common criteria in security risk assessments.[659] The first component is an asset and refers to any tangible or intangible object that is valuable for a company, such as primary assets like information, data, and supporting assets like IT systems, facilities, networks and people. The second component is a threat, a term which denotes a future event (action or inaction) that can lead to an undesirable situation. ENISA created a threat taxonomy, which illustrates a multitude of possible security threats, ranging from physical attacks on IT assets, natural disasters, outages and system or device failures to individual nefarious cyber-activities.[660] The most frequent cyber-threats, for example, in the last year were malware, web based and application attacks, and botnets.[661] The third component is vulnerability, a weakness in an asset or a factor that increases the probability or likelihood of the threat being successful. Examples of vulnerabilities may include (in line with the above-mentioned threats) unprotected public network connections, locations vulnerable to flooding, equipment sensitive to changes in

---

[656] Some sources distinguish more properties of information to be preserved, for example Regulation 526/2013 specifically in data rather than information security context refers in addition to "authentication" and defines all characteristics as follows: "availability" means that data is accessible and services are operational; "authentication" means the confirmation of an asserted identity of entities or users; "data integrity" means the confirmation that data which has been sent, received, or stored are complete and unchanged; "data confidentiality" means the protection of communications or stored data against interception and reading by unauthorised persons. See article Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, L 165/41, 18.6. 2013. Also ISO standards mention other additional possible information characteristics to be protected: authenticity ("property that an entity is what it claims to be"), accountability, non-repudiation ("ability to prove the occurrence of a claimed event (…) or action and its originating entities"), reliability (property of consistent intended behaviour and results").

[657] ISO/IEC, "Information technology -- Security techniques-Information security risk management" ISO/IEC FIDIS 27005:2008 "*the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the probability of occurrence of an event and its consequence".*

[658] John Vacca, Computer and Information Security Handbook, 2nd Edition, 2013, p. 907.

[659] For an overview of formal information security-related definitions used in the ISO27k standards see ISO/IEC 27000:2016 (E) Information technology — Security techniques — Information security management systems - Overview and vocabulary (fourth edition) for an overview of information security management related terms, at: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

[660] ENISA, Threat Taxonomy, A tool for structuring threat information, at: January 2016, ttps://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information

[661] For the latest yearly report, see ENISA Threat Landscape 2015, at: https://www.enisa.europa.eu/publications/etl2015

voltage and a lack of identification and authentication systems. The last core component is the impact on the asset if the threat exploits the vulnerability, such as the (potential) loss or damage when the negative event happens.

Theoretically, numerical values, such as monetary expression of impact and probability calculations for other elements, can be assigned to the risk element.[662] This facilitates a cost-benefit analysis and hence a comparison of the risk with the cost of the adopted security measures. However, expression of risk in monetary value raises significant concerns, as it is difficult and undesirable to express some assets, like human life, in economic terms.[663]

International and national standards on information security management all employ the specific above-mentioned terminology related to the central concepts of threat, vulnerability, and impact. However, this terminology which coincides with the interest of the company to protect its assets, does not entirely correspond to the needs of data protection law to assess the impact on the rights and freedoms of individuals whose data are processed, as envisioned in the GDPR. There are several reasons for this mismatch. First, the rights and freedoms of individuals can hardly fit into the corporate conception of an asset to be safeguarded, along with hardware, software, or networks. That being said, company reputation or trust of the users can nevertheless be important and provide an incentive to process personal data in line with the expectations of the users. Also, while security threats are posed by outsiders (e.g. hackers, natural disasters) or insiders (e.g. employees) in relation to personal data protection, the major sources of threats are often the companies and their business models themselves. Companies take strategic decisions regarding how much personal data to collect, how long to keep it, how to create data flows and transfers, which technologies and security measures to use. Second, according to Vacca, in the information security field "risk can be reduced by applying security measures; it can be shared by outsourcing or by insuring; it can be avoided; or it can be accepted, in the sense that the organization accepts the likely impact of a security incident."[664] The idea of insuring or accepting the negative impact on the rights and freedoms of individuals is not easy to accommodate within the human rights discourse. Cost-benefit calculations are also at odds with the protection of human rights and it is not clear how risks to individuals should be weighted with the benefits of the processing. Third, harms from security breaches are well defined and understood, but this understanding is lacking around privacy harms. For the privacy engineering objectives to mitigate the risk of privacy harms, such harms need to be clearly explicated.[665] Yet, privacy harms might be more difficult to recognise and control than security harms. Privacy harms "may arise even though the system is performing data actions in accordance with its operational purpose", for example beyond harms arising from malicious actors or attacks, and privacy harms "may occur externally to the system, and beyond the system owner's awareness"[666].

Despite the divergence in data security and privacy domains, there have been efforts to partially adapt and apply technical data security terminology to assess privacy risks for data subjects. On a high level, international standards such as the ISO Privacy Framework adds to the data security a focus relevant to personal data processing. [667] Several works have tried to operationalize privacy in the context of information security. In the PRIAM report, for example, computer scientists expanded the well-established notions in data security in order to

---

[662] Ibid.

[663] John Vacca, Computer and Information Security Handbook, 2nd Edition, 2013, p. 907.

[664] Ibid.

[665] NIST Privacy Engineering Objectives and Risk Model Discussion Draft, *p. 3, footnote 9.*

[666] NIST Privacy Engineering Objectives and Risk Model - Discussion Deck Objective-Based Design for Improving Privacy in Information Systems, 2014, at http://csrc.nist.gov/projects/privacy_engineering/nist_privacy_engr_objectives_risk_model_discussion_deck.pdf, p. 13.

[667] ISO/IEC 29100 Privacy framework, 2011.12.15

account for threats that can lead to privacy harms and included privacy harms, which they derived from the feared events and external factors, such as social norms, laws, among the privacy risks assessment criteria.[668] The CNIL similarly in trying to help the use of a EBIOS software tool developed by Central Information Systems Security Division in France for risk analysis and management in the specific context of personal data protection adapted the information security concepts to the personal data protection area. It views risk as consisting of "a feared event and all the threats that may allow it to occur" and focusses on the protection of personal data supporting assets.[669] Most extensively, in the US, similar to the CIA triad, NIST created privacy engineering objectives underlining core characteristics of systems to implement measurable control for assessing privacy risks.[670]

The logic and aim of the information security management is reflected in Article 17 of the Directive 95/46/EC. It embodies the requirement for data controllers to adopt technical or organisational data security measures to protect personal data against "accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access", i.e. respectively guarantee data availability, integrity, and confidentiality. This general requirement does not refer to a specific risk definition and its assessment methodologies, but mentions risk as one of the criteria to judge the appropriateness of data security measures. According to the wording of Article 17, data controllers are obliged to guarantee technical and organizational security measures 'appropriate to the risks represented by the processing and the nature of the data to be protected'. Thus, although it is not explicitly specified, the Directive requires, first, to know the risks posed by particular data processing operations and, second, based on this knowledge to determine adequate security measures that prevent or diminish possibilities of unlawful data processing activities. In other words, security measures should be systematically prepared to avoid unlawful data processing tailored to the risks that a particular processing operation entails, based on so called risk reduction principle.[671] In this respect, risk is a determinant factor for application of adequate (depending on the given situation) security measures.

3.2.2. Risk as an obligation adjuster

In the Data Protection Directive, risk has been used to steer the way in which Member States are to make use of their discretion to adjust legal duties and obligations of data controllers in their national laws in relation to the notification procedure (Article 18)[672], prior checking procedure (Article 20), and the exemption from an obligation to provide access to personal data in specified cases (Article 13). First, the Directive establishes a general requirement of notification about personal data processing to the supervisory authority, which aims to ensure that the purposes and the main features of data processing operations are public and open for verification. However, 'in order to avoid unsuitable administrative formalities' (Recital 49), the Directive uses 'risk' as a criterion to be considered by the Member States when deciding whether certain data controllers can be exempted from or be subject to simplified notification procedure. This could be the case 'where processing is unlikely adversely to affect the rights and freedoms of data subjects' taking account of the personal data to be processed, or where an independent data protection official 'ensures that the processing

[668] Sourya Joyee De, Daniel Le Métayer. PRIAM: A Privacy Risk Analysis Methodology. [Research Report] RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes (2016) <hal-01302541>;

[669] CNIL, Privacy Impact Assessment (PIA), Methodology (how to carry out a PIA), June 2015 edition, https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

[670] http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf p. 17

[671] Ulrich Dammann, Spiros Simitis, *EG-Datenschutzrichtlinie:Kommentar* (1 ed., Baden-Baden, Nomos, 1997) Art. 17.7.

[672] Article 18 does not mention the word „risk' as such, but refers to it as a likelihood of adverse effect to the rights and freedoms of data subjects.

carried out is not likely adversely to affect the rights and freedoms of data subjects' (Recital 49). In other words, Member States are given considerable room for manoeuvre to exempt controllers from the notification duty or simplify it if the risk associated with the processing is low. For example, many Member States exclude standard processing operations relating to internal administrative purposes (salary and personnel administration, accounts records, or data on customers, suppliers and membership) on the condition that they are carried out in accordance with specific legal rules as such low risk processing.[673] In general, however, the lists of national exemptions from notification procedure differ significantly in their scope and specific requirements among the Member States.[674]

Second, the Data Protection Directive recognizes that some – according to the text a limited number - of data processing operations pose more specific risks to data subjects than others. Therefore, they cannot start without prior checking of the national supervisory authority. Based on the examination, the supervisory authority may give an opinion or an authorization regarding such, supposedly more risky, processing activities. According to the text of the Directive, decisive elements showing that certain operations pose higher risk to the rights and freedoms of individuals are: 'their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract' or 'the specific use of new technologies' (Recital 53). Practical examples that the Member States determined as likely to present specific risks to the data subjects and thus are subject to prior checking often include sensitive data, processing related to interconnection of databases, credit referencing, or the use of new technologies to carry out data processing.[675]

Third, risk justifies the exceptions to the rights of access of data subjects (Article 13(2)) that might be introduced by Member States if the processing occurs for the sole purpose of scientific research or the creation of statistics, when 'where there is clearly no risk of breaching the privacy of the data subject'. Such an exception should be subject to adequate national legal safeguards, especially the data cannot be used for taking measures or decisions regarding any particular individual.

3.2.3. Risk as a regulatory object delineator

Risk has been implicitly used to define the object of data protection law as conceptually it is a criterion to categorize personal data as 'sensitive' or 'ordinary' (Article 8) and to treat the processing of the former more rigidly. The rationale behind the categorisation is based on the understanding that although normally the harm that can be caused to privacy depends on the context in which data are processed rather than on the content of the data as such,

---

673 Douwe Korff, EC Study on Implementation of Data Protection Directive (Study Contract Etd/2001/B5-3001/A/49) Comparative summary of national laws, 2002, at http://194.242.234.211/documents/10160/10704/Stato+di+attuazione+della+Direttiva+95-46-CE

674 European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003, COM/2003/265 final (First Implementation Report). Communication on the follow-up of the Work programme for a better implementation of the Data Protection Directive, 7 March 2007, COM (2007)87 final (Second Implementation Report). Annex 2 to the Impact Assessment, Accompanying the General Data Protection Regulation and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, Brussels, 25 January 2012 SEC(2012) 72 final (Third Implementation Report).

675 Douwe Korff, EC Study on Implementation of Data Protection Directive (Study Contract Etd/2001/B5-3001/A/49) Comparative summary of national laws, 2002. For a detailed overview of the operations subject to prior checking in different EU Member States see Gwendal Le Grand , Emilie Barrau, Prior Checking, a Forerunner to Privacy Impact Assessments in David Wright, Paul De Hert (eds.), Privacy Impact Assessment, Volume 6 of the series Law, Governance and Technology Series, 2012, pp 97-116

nevertheless, 'certain categories of data do by their nature pose a threat to privacy'.[676] In this sense, there is an *a priori* presumption of riskiness in relation to sensitive data and independently of the actual context the legislator relies on precautionary principle as to its processing. Special attention to sensitive data follows the logic of higher, particularly adversary or discriminatory, effect that processing of sensitive data can have to individuals, groups or society as a whole. Indeed, sensitive data are referred to as the area where the main privacy concerns would normally lie[677] or named as ''hard core' of the private life'.[678] Sensitive data pertain to the very private or intimate aspects of one's life, like racial or ethical origin, religion, political, philosophical or ethical persuasions, trade-union membership, health, sexual life.[679] However, as claimed by Poullet: 'it is not the privacy – a vague and undefinable concept – but the fear of discriminatory practices which justified the severe restrictions a priori on the collection storage of such data'.[680]

3.3. General Data Protection Regulation (2016/679)

In the General Data Protection Regulation, increased number of data protection provisions have been built around the concept of risk. This risk-based turn, to a large extent, can be explained not only by the aim of compliance cost reduction and efficiency, but also by the need to ensure greater harmonisation and greater consistency of the data protection across the EU. The Regulation as a directly applicable legal instrument can no longer declare that risk should be used as a yardstick to adjust data controllers' obligation by Member States, as did the Directive, but actually has to specify the calibrated obligations in its text itself.[681]

3.3.1. Risk as a core of the accountability principle

In contrast to five references to risk in the Data Protection Directive, in the General Data Protection Regulation the term risk is spilled out over the whole text. Most importantly, risk becomes a core element of the accountability (responsibility) principle and risk management is at the center of the data protection impact assessments, a new tool that helps to achieve and demonstrate compliance with the Regulation. As noted by Spina, such assessments become the "new enforced self-regulation model" through which risk control is materialising.[682] Article 24, on the responsibility of the controller, sets forth that 'taking into

---

[676] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Amended Proposal'), COM (92) 422 final—SYN 287, 15 October 1992. It can be accessed on the Archive of European Integration of the University of Pittsburgh <http://aei.pitt.edu/10375>.

[677] Paul De Hert, Vagelis Papakonstantinou, 'The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals' (2012) 28(2) Computer Law & Security Review 130-142.

[678] Yves Poullet, 'Data Protection between Property and Liberties – A Civil Law Approach' in Guy P. V. Vandenberghe, H.W.K. Kaspersen, Ania Oskamp (eds), *Amongst Friends in Computers and Law: A Collection of Essays in Remembrance of Guy Vandenberghe* (Kluwer Law & Taxation Publishers, Deventer / Boston 1990) 161-181, 163.

[679] The notion 'Sensitive data' is changed to 'Special categories of personal data' in the Regulation and is meant as personal data 'revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.

[680] Yves Poullet, Data Protection between Property and Liberties (supra note) 163.

[681] Quelle, Claudia Quelle, The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too, 2017.

[682] A. Spina (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. European Journal of Risk Regulation, 8(1), 89-90.

account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures', including appropriate data protection policies, to achieve compliance with the Regulation. This article goes beyond the data security measures and refers to all the measures necessary to comply with the data protection principles, meet all obligations stemming from the Regulation, and be accountable according to Article 5(2). It allows scaling (but not eliminating) data processors' obligations and accountability according to the risks posed by the relevant processing operations. As explained by Hustinx "more detailed obligations should apply where the risk is higher and less burdensome obligations where it is lower".[683] The rights of the data subject, however, are not called into question and must be guaranteed by data controllers, whatever risks are posed to data subjects.[684] Equally, data controllers remain accountable regardless of the risk involved.[685]

Despite the apparent clarity that the risk-based approach in the GDPR refers to nothing more than scalable and proportionate compliance, it is debatable what the real impact of the risk-based provisions will be in practice.[686] The Article 29 Working Party does not provide any clarity but rather complicates the answer by putting forward the following statements: controllers remain always accountable for the GDPR compliance, but there are different levels of accountability obligations depending on the risks; fundamental data protection principles applicable to the controllers are the same independently from risks, but these principles are inherently scalable.[687] Given the possibility to scale the majority of the GDPR provisions, it remains debatable whether any of the GDPR rules are completely immune from the risk-based approach.

3.3.2. Risk as a trigger of new obligations

The Regulation not only further extends the same reference to risk in relation to data security as in the Directive 95/46/EC, but also involves risk in the context of new obligations, such as an obligation to keep records of processing activities (Article 30), and to observe the principle of data protection by design and by default (Article 25). Rather than tailoring the scope of the obligations, risk and its level triggers the applicability of some new requirements which become obligatory to data controllers only if their processing activities pose a risk or a high risk to data subjects (Data Protection Impact Assessments (Article 35), appointment of a data protection officers (Articles 37-39), and data breach notifications (Article 33-34)).

IV. The Second Shift – The GDPR and Risk Regulation

As the analysis above demonstrates, risk has gained a number of new manifestations with the implementation of the risk-based approach in the General Data Protection Regulation. Yet, in addition to tailoring compliance to risk, the GDPR seems to contain a number of more

---

683 Peter Hustinx, EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation, 2014, p. 20, 38, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2014/14-09-15_Article_EUI_EN.pdf

684 Ibid.

685 Article 29 Data Protection Working Party, Annex to the Letters from the Art. 29 WP to LV Ambassador Ilze Juhansone, MEP Jan Philip Albrecht, and Commissioner Vĕra Jourová in view of the trilogue (17 June 2015), 15.

686 See Claudia Quelle, The 'risk revolution' in EU data protection law: we can't have our cake and eat it, too, 2017.

687 Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', WP 218, 30 May 2014.

structural elements and mechanisms present in risk regulation, ranging from the risk scoring and assessing systems, the institutional arrangements and to public participation in risk regulation.

4.1. System for assessing and scoring risks

In the risk regulatory frameworks regulators develop a system that allows them to measure and score identified risks.[688] In such risk-scoring systems, risk typically is viewed as 'the product of the gravity of a potential harm or impact and the probability of its occurrence'.[689] There may be various ways of measurement, in some countries predominantly qualitative or in contrary quantitative, but in essence the measurements will be based on the elements of quantum and probability.[690] Most often numerical scores would be assigned and categorisation such as 'high', 'medium', 'low' risks would be used.

If we look to data protection law, except for the national guidelines adopted by the UK, French and Spanish data protection authorities,[691] there are no uniform risk measurement and scoring systems. The situation has changed somewhat with the General Data Protection Regulation. Severity and probability as important risk measurement elements receive more intentional focus in the Regulation. Recital 76 states that the likelihood and severity of a risk "should be determined by reference to the nature, scope, context and purposes of the processing" on the basis of an objective assessment. The assessment should establish whether a risk or a high risk exists to the rights and freedoms of natural persons. The Article 29 Working Party has also recently recognised that the severity of risk and the likelihood of negative impact should be taken into account while evaluating the risks for individuals' privacy.[692] Although there is not yet a uniform system for assessing and scoring risks to the rights and freedoms of data subjects, there is a clear tendency to subject risk in the area of data protection law to quantification and measurement. The Article 29 Working Party in its recent guidelines has recognised that various methodologies can be used by data controllers to assess risks as long as they meet the standards of the GDPR, i.e. provide a description of the processing operations and their purposes, assess the necessity, proportionality, and the risks to the rights and freedoms of data subjects, foresee the measures to address the risks.[693]

One further step which is often made by regulators in relation to the seriousness assigned to risks, is the prioritisation of the higher risk producers for attention and intervention.[694] This is not yet reflected in the legal data protection framework, or at least officially the enforcement of data protection law is not related to risk in the General Data Protection Regulation. In practise, though, on a national data protection authority (DPA) level, risk is already has been shaping the way in which public supervisory functions are performed.

---

688 Robert Baldwin, Martin Cave, Martin Lodge, 282.

689 Ibid.

690 Julia Black, 'Risk Based Regulation: Choices, Practices and Lessons Being Learned' in *Risk and Regulatory Policy: Improving the Governance of Risk* (OECD, 2010).

691 Information Commissioner's Office, 'Conducting Privacy Impact Assessments' (2014) Code of Practise <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf >; Agencia Espanola de Proteccion de Datos, 'Guía para una Evaluación del Impacto en la Protección de Datos Personales' (2014) <http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf>. Commission Nationale de l'Informatique et des Libertés (CNIL), Privacy Impact Assessment (PIA) Methodology (how to carry out a PIA), (2015) < https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf >

692 Article 29 Data Protection Working Party, Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks, 4.

693 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4 April 2017.

694 Robert Baldwin, Martin Cave, Martin Lodge 282.

The risk-based approach in some Member States is seen as providing a more effective and efficient way to handle data subjects' complaints, check compliance with data protection law and, as a result, to better use the limited resources assigned to the DPAs. Risk as a driving factor to prioritize and select complaints to be handled is already present in the working practice of several DPAs to a certain extent. For example, the Dutch DPA selects complaints to be handled on the basis of five criteria: 1) serious violations; 2) structural violations; 3) violations that concern many people; 4) violations where the Dutch DPA can effectively intervene with its enforcement instruments; 5) violations that occur within the (annual) focus.[695] Similarly, the ICO in the UK has recently taken a new approach and started focusing on systematic issues and patterns of poor behaviour of organizations rather than on each and single individual case.[696]

Although the current European data protection system does not have a uniform framework to measure and score identified privacy risks, some changes in this respect are happening. Severity and probability are inserted into the General Data Protection Regulation as important risk measurement elements. There is an EU-level agreement between the DPAs that different types of risk assessment frameworks can be used by data controllers, given that they satisfy the main GDPR standards. Yet, as it will be discussed below, some of the risk assessment frameworks can arguably be better equipped to assess risks than others.

4.2. Institutional arrangements

In traditional risk regulation domains, a well-established division between risk assessment, a scientific process, and risk management, a purely political process, exists.[697] Since the 1990s, the EU also has tried to separate the scientific risk assessment and the political process of risk management in regulation of risks to human health, safety and the environment. This effort has led to a process of institutionalising risk assessment tasks and the so called 'mushrooming' of specialized European agencies.[698] Risk assessment in relation to the environment, chemicals, pharmaceuticals and food is formally dedicated to the respective regulatory agencies namely, the European Environment Agency, the European Chemicals Agency, the European Medicines Agency, and the European Food Safety Agency.
Decisions about risk management remain within the discretion of the European Commission and other EU institutions. This is a way to 'disentangle scientific risks assessment from political risk management'[699] and to grant more legitimacy to the EU policy-making, even if in the daily practise the separation the two aspects is not so clear-cut.[700] Normally, a regulatory agency is defined as an independent 'administrative organization with a distinct, formal identity, an internal hierarchy, functional capacities, and, most important, at least one principal'.[701]

---

[695] Dutch Data Protection Authority, Beleidsregels handhaving door het CBP (DPA policy rules for enforcement) (2011) https://cbpweb.nl/sites/default/files/atoms/files/beleidsregels_handhaving_cbp_0.pdf accessed 14 February 2015.

[696] The new approach of Information Commissioner's Office (UK) (taken as from 1 April 2014) as regards its supervisory powers is described in Public Consultation paper 'Our new Approach to Data Protection Concerns' (2013) <https://ico.org.uk/media/about-the-ico/consultations/2019/a-new-approach-consultation.pdf> accessed 10 February 2014.

[697] Julia Black, 311.

[698] Govin Permanand, Ellen Vos, 'EU regulatory agencies and health protection', in Elias Mossialos and others (eds) *Health Systems Governance in Europe* (Cambridge University Press, New York 2010) 134-186, 134.

[699] Julia Black, 311.

[700] Ibid.

[701] David Levi-Faur 'Regulatory networks and regulatory agencification: towards a Single European Regulatory Space' (2011) 18(6) Journal of European Public Policy 810-29, 813.

Attributed with special, less political, but more technical and scientific tasks, such specialised agencies differ from the EU institutions.

A similar tendency to 'depoliticize' risk assessment processes assigning this role to an independent and technical body can be noticed in the GDPR. The main expert body under the Data Protection Directive is a Working Party on the Protection of Individuals with regard to the Processing of Personal Data (hereinafter – the Article 29 Working Party). It acts independently based on its own rules of procedure and has an advisory status. It is a formal network composed of established independent national data protection authorities, the European Data Protection Supervisor and the European Commission. The Article 29 Working Party elects its temporal Chair and two Vice-Chairs by means of a secret ballot for a term of two-years.[702] The main functions of the Working Party are: to examine any question related to the uniform application and amendments of the Data Protection Directive, to advise the European Commission on the level of data protection in the EU and in third countries, and to issue opinions on European codes of conduct.[703] The Article 29 Working Party has already started providing guidelines on high risk data processing operations, i.e. defining and partially assessing risks to the data subjects stemming from data processing operations.[704]

The General Data Protection Regulation transformed the Article 29 Working Party to an independent European Data Protection Board. There are at least three new aspects in relation to its formation, structure, and tasks that are worth noting. First, the composition of the group changes slightly but significantly. The European Data Protection Board formally consists of a head of a supervisory authority of each Member State and of the European Data Protection Supervisor. Differently from the Article 29 Working Party, the Commission can only participate in the Data Protection Board's activities without a voting right (Article 68.5). This participatory right even totally disappeared in the amendments of the European Parliament, but has been restored in the final text of the Regulation. This shows a clear will of the Parliament members to eliminate any political 'flavour' and to create a specialised, independent, knowledge-based entity.

Second, the secretariat previously provided by the European Commission has now been placed within the European Data Protection Supervisor (EDPS) (Article 75). The Commission justified this change with the aim 'to provide a strong basis for cooperation among data protection authorities, including the European Data Protection Supervisor' and 'to enhance synergies and effectiveness'.[705] In order to fully understand the implications of this change, the status and role of the EDPS should be first clarified. The EDPS, contrary to the European Commission, is a specialised and politically independent EU office, with the main objective to ensure that EU institutions and bodies respect the right to privacy while processing personal data and developing new policy instruments, rules laid down in Regulation (EC) No 45/2001.[706] Among other functions, the EDPS monitors the processing of personal data in the EU administration and ensures compliance with the data protection rules, advises the EU institutions on new legislative proposals, and cooperates with other data protection authorities

---

[702] Ibid.

[703] Article 29 Data Protection working Party, 'Rules of Procedure of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data', 15 February 2010 < http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/rules-art-29_en.pdf> accessed 10 February 2015

[704] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4 April 2017.

[705] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century, COM/2012/09 final.

[706] Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12 January 2001.

through the Article 29 Working Party. As a result, this change means that the Article 29 Working Party from politically imbedded, even if composed of independent national data protection authorities, becomes increasingly institutionalised and formalised, with its own distinct legal personality. The European Commission loses the right to formally be a member of this new structure and have any influence through hosting its activities.

Third, with the GDPR the decision power of the European Data Protection Board increases and becomes binding. As its predecessor, the Board maintains the consultative role. From advising the Commission to adopting guidelines for the purpose of specifying a high number of articles in the Regulation or encouraging consistent application of any other relevant GDPR provision on its own initiative. These wide powers are the result of the Parliament's decision to diminish the discretion that the European Commission granted to itself in 26 instances to supplement the GDPR by delegating acts and represent the shift of power away from the Commission to a politically independent body.

Even more importantly, the role of the Board is made central and decisions binding in the consistency mechanism. Before a DPA adopts an important decision, it must first obtain an opinion of the Board (Article 64). One of these such decisions is the list of the processing operations subject to the requirement for a data protection impact assessments, i.e. definition of the high risk data processing operations.[707] The DPA should "take utmost account of the opinion of the Board" and inform how it is reflected in the draft decision (Article 64.7). When the DPA does not follow the opinion of the Board, in order to ensure the correct and consistent application of the GDPR, the Board adopts a binding decision (Article 65). In the same vein, the Board acquires binding decision making power in case of disagreement between the DPAs, as opposed to the non-binding merely authoritative nature of the Article 29 Working Party opinions. In applying the consistency mechanism, the European Data Protection Board is empowered to issue an opinion or to adopt legally binding decisions in clearly specified cases where there are conflicting views or disputes among supervisory authorities by a two-thirds majority of its members, in particular deciding whether there is an infringement of the GDPR. The Board thus becomes "the highest executive data protection monitoring party in the EU", that is "capable of deciding on itself and enforcing its opinions".[708]

In sum, the General Data Protection Regulation introduces major changes in relation to the formation, tasks and structure of the main European data protection expert body - the Article 29 Working Party. The European Data Protection Board compared to its predecessor is completely 'depolitizised', institutionalised and its functions are extended to include binding decision making. Creation of this specialised, independent, knowledge-based entity partially denotes a shift toward independent, scientific risk assessment in data protection.

4.3. Public engagement in risk regulation

Engaging stakeholders and the general public into risk management process is a well acknowledged necessity in risk regulation. The mere fact that the aim of the risk-based regulation to manage contestable risks, opens the door for society to participate in the understanding and formulation of risks.[709] This is not the case in relation to the regulation defined in terms of the market or human rights.

---

[707] Article 29 Working Party has already started providing guidelines on high risk data processing operations see Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4 April 2017

[708] Paul de Herta, Vagelis Papakonstantinou, The new General Data Protection Regulation: Still a sound system for the protection of individuals?, Computer Law & Security Review, 32(2), 179-194, 193.

[709] Julia Black, 309.

There is a wide acknowledgment of the benefits that public participation can have to risk identification and management. These include the help of the stakeholders to discover risks that otherwise may 'fly under the radar' of the assessor, provide input on the perceptions of the severity of risks and on possible ways to mitigate them.[710] If the data protection impact assessment (DPIA) is meant to be more than a mere compliance check with the data protection rules, it should engage stakeholders in identifying and assessing risks and impacts.[711] The ICO PIA Handbook recommends stakeholder engagement.[712] It also states that wider consultation of affected individuals is important not only because "it enables an organisation to understand the concerns of those individuals" but also it "improve(s) transparency by making people aware of how information about them is being used".[713] As Roger Clarke noted, 'the objectives of a PIA cannot be achieved if the process is undertaken behind closed doors. In a complex project applying powerful technologies, there are many segments of the population that are affected. It is intrinsic to the process that members of the public provide input to the assessment, and that the outcomes reflect their concerns.'[714] In the same vein, "In the same vein, Wright and Mordini claim that given the right to good administration enshrined in Article 41 of the Charter of Fundamental Rights of the European Union, consultation with stakeholders in the process of the DPIA "is not only desirable but necessary".[715]

For the first time the Regulation makes an effort to involve the stakeholders and the public at large in to the actual process of risk evaluation. Article 35.9 of the General Data Protection Regulation requires, where appropriate, to 'seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.' One would, indeed, expect those who are to be effected, i.e. the end users, to be in the best position to articulate their fears and negative possible effects of the particular technologies or systems. In practice, however, this requirements is a soft obligation. As public engagement might be related to individualised risks assessment and high costs for companies, it is not surprising that the obligation to take individual views into account is seen as hardly achievable in all the cases and thus applicable only 'where appropriate'. The 'appropriateness' standard is not defined in the Regulation and thus is left to the discretion of the data controllers. Moreover, data controllers are exempted from the obligation to consult with data subjects when there is a need to protect their commercial interests. This need might be less pressing and obvious for the projects and systems in the public sector, but private companies might try to retain business secrets from the beginning of the development of their new products and services in order to gain competitive advantage.[716] Therefore, it is questionable to what extent they will be willing to

---

[710] David Wright, Emilio Mordini, 'Privacy and Ethical Impact Assessment' in David Wright and Paul de Hert (eds), *Privacy Impact Assessment* (Springer, Netherlands 2012), 397-418, 402.

[711] David Wright and others, A Privacy Impact Assessment Framework for data protection and privacy rights, PIAF project Deliverable D1 (2011), A Report of the PIAF Consortium Prepared for the European Commission, <www.piafproject.eu> accessed 10 February 2015. (The report states: "A PIA is more than a check that a project complies with existing legislation and privacy principles. A PIA should include compliance check, but it should go beyond a simple compliance check and engage stakeholders in identifying risks and privacy impacts that may not be caught by a compliance check", 189)

[712] Information Commissioner's Office, 56-58.

[713] Ibid., 18.

[714] Clarke Roger, 'PIAs in Australia: A work-in-progress report', in David Wright and Paul de Hert (eds), *Privacy Impact Assessment* (Springer, Netherlands 2012).

[715] David Wright and Emilio Mordini, "Privacy and Ethical Impact Assessment" in David Wright and Paul de Hert (eds), Privacy Impact Assessment (Springer, 2012) 397, 402.

[716] David Wright, Raphaël Gellert, Serge Gutwirth & Michael Friedewald, Precaution and privacy impact assessment as modes towards risk governance in René von Schomberg (ed.), Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields, A Report from the European Commission Services, available at: http://philpapers.org/archive/VONTRR.pdf

disclose detailed information about the data collection practises and projects and involve a wide range of relevant stakeholders. In addition, the Regulation requires the views of the data subjects to be heard but does not oblige controllers to take these views into account or to implement changes following data subjects' suggestions. Thus, ultimately stakeholder consultation is purely of an informational nature and neither provides assurances of comprehensive risk identification nor guarantees a full-pledged protection from risks.
Besides the DPIA, there is also an additional tendency in the Regulation to engage with the public concerning risks. Education, training and communication is seen as a core aspect of the regulatory function. Risks are to be made intelligible to non-specialists as according to the General Data Protection Regulation each supervisory authority shall 'promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing' (Article 57.1.b).

In sum, the effort to include data subjects and their representatives in the risk management process proposing a separate article on this in the General Data Protection Regulation would provide a possibility for external stakeholders and the public to participate in defining risks and deciding on their impact in data protection law. On a practical level, however, there are debates on how data subjects and other stakeholders could have a say in the related data protection risk assessments. First emerging considerations demonstrate not only the early stage of reflections on the public involvement in the privacy impact assessments, but also possible difficulties to achieve such involvement in practise. For example, as queried by the Centre for Information Policy Leadership: 1) should data subjects be allowed to participate directly in the risk assessment or just get access to its findings?; 2) should (and if so how should) companies can take into account individuals' perception of risk and harm in practise, e.g. through monitoring their opinions via social media?[717] It has been suggested that risk assessment should be based on objective characteristics of harm and examine 'harm imposed on the reasonable man or woman' in a particular context: 'in the same way as tort law ignores the 'egg shell skull', the test is not and cannot be, concerned with the impact on each particular individual, let alone an individual with particular sensibilities.'[718] Similar positions appear to be delineated in the Regulation (Recital 76), which requires data controllers to carry out an 'objective' risk assessment.

V. Reflections on the Two Shifts

The two shifts present a number of unresolved challenge with the nature of an individual fundamental right of data protection. This sections focuses on three of them – the difficulty to align the risk with rights regulation due to data protection foundations, unjustified faith in self-regulatory enforcement of data protection rules, and undefinable and unmeasurable risk as a core element of the shifts.

(they claim "companies are not obliged to be as "democratic" and participatory as governments in developed countries have to be. And the involvement of stakeholders in the development is notoriously difficult and costly even if the products, services or policies have the potential for intrusion on privacy or are ethically dubious. Furthermore, competition in the private sector, especially in the development and promotion of new products and services, often involves secrecy in the early stages.", 95)

717 Centre for Information Policy Leadership, 'A Risk-based Approach to Privacy: Improving Effectiveness in Practice' (2014) <http://www.hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf> accessed 20 June 2017.

718 Ibid, 7.

5.1. Data protection law and its foundations

Historically, risk regulation is known as regulation that tackles the risks related to human safety, health and the environment. Several main elements of risk regulation have been distilled in the regulatory literature. First, the ultimate aim of risk regulation is 'to control relevant risks, not to secure compliance with sets of rules'.[719] Thus, regulators should establish clear objectives and the risks that those regulated pose for the achievement of these objectives.[720] In the mid-90's, European data protection legislation emerged as a regulatory effort aiming to protect individuals with regard to the processing of personal data while at the same time allowing free data flows. In essence, the regulatory goal was to protect individuals against the misuse of their personal data, and thus against violations of their privacy and other rights, which initially revolved mainly around data security-related concerns.[721] Such protection of human rights was envisioned through securing compliance with specific data protection principles and provisions rather than through the control of data processing-related risks. The Directive 95/46/EC does not even refer to concrete risks to privacy and personal data protection and avoids explicit references to three classical steps of the risk analysis framework (risk assessment, management and communication). The General Data Protection Regulation comes closer to the classical risk regulation concept, as it names a number of specific risky data processing activities (Article 35(3)) and possible damages to individuals (Recital 85). The latter include physical, material or non-material damage to such as loss of control over one's personal data or limitation of one's rights, discrimination, identity theft or fraud, financial loss, damage to reputation. Yet, the risks remain defined in a flexible and abstract way and need to be specified and assessed by data controllers depending on the particularities and specificities of each data processing case.

Second, and even more importantly, risk regulation is focused on (potential) 'harm' and 'negative consequences' to individuals or to the environment. For example, as stated by the aim of much modern environmental law is "to prevent harm to the environment before it occurs, with an implementation structure that includes prior approvals, permits that embody standards to be met, and the monitoring of compliance, all with that goal in mind."[722] Data protection law has a broader aim than just protecting an individual from harm through risk control and mitigation. The right to data protection is safeguarded regardless of harms or possible adverse effects on individuals.[723] Lynskey claims that 'there is a general interest in conferring control

---

[719] Robert Baldwin, Martin Cave, Martin Lodge, *Understanding Regulation: Theory, Strategy and Practise* (2 ed., Oxford University Press, New York 2012) 281.

[720] Ibid. 281-282.

[721] Although the goal of the EU Data Protection Directive is not framed in terms of addressing risks to privacy, the goal of other data protection laws and statutes, e.g. the first data protection legislation of the German Lander of Hesse or 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, may be considered to address the risks to privacy stemming from the development of new technologies. See Viktor Mayer-Schönberger, "Generational Development of Data Protection in Europe." In *Technology and Privacy: The New Landscape*, Eds. Agre, Phillip E. and Marc Rotenberg. Cambridge, MA: The MIT Press, 1997, 219-242 (he states that the first data-protection laws were enacted in response to the emergence of electronic data processing within government and large corporations and the plans to centralize all personal data files in gigantic national data banks). Raphaël Gellert, 'Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative' (2015) 5(1) International Data Privacy Law, *3-19* (he claims that the explicit object of many data protection statutes is to address the 'risks to privacy' stemming from the development of ICTs).

[722] Donald K. Anton, Dinah L. Shelton, Environmental Protection and Human Rights (Cambridge University Press, 2011), 38.

[723] Lynskey, Orla (2015) The foundations of EU data protection law, Oxford studies in European law (Oxford University Press, 2015).

over personal data to individuals even in the absence of tangible or intangible harm' and it can be comparable to the protection of other general interests, such as the protection of liberty.[724] Also, several normative values underlie the fundamental right to data protection: autonomy, informational self-determination, balance of powers, integrity and dignity.[725] The majority of data protection laws identify privacy as the main justification for their adoption.[726] Privacy plays an instrumental role in protecting individual's interests, such as autonomy, welfare, equality, justice, dignity, status, tranquillity, [727] and freedoms, such as freedom of expression, and violations of privacy can harm their enjoyment.[728]

European data protection law, therefore, being a fundamental rights (sui generis) regulation, is built on different foundations than risk regulation. The possibility to reconcile or align the risk with rights regulation is contested and presents complex questions, which fall outside the scope of this article. A pure risk regulation and risk-based approach would not sufficiently protect the right to data protection because 'it would presuppose the legality of data processing activities regardless of individuals' fundamental rights'.[729]

5.2. Shifts towards risk as a response to a regulatory crisis

Reliance of risk in regulation can be seen as a way to bridge the gap between law and technological developments. Data protection law is known for the disconnect between law in the books and law in action.[730] It is not able to catch up with the rapidly evolving technologies and ubiquitous data collection. It can no longer give control over their personal data to individuals in the era of profiling, and Big Data, and address all the negative impacts stemming from the collection and use of data on data subjects.[731] Any regulatory response to the new socio-technological challenges has its clear limits. On the one hand, the reliance on high-level principles renders it difficult to address and solve the actual problems, i.e. to focus on the objectives of data protection.[732] On the other hand, including more and more concrete types of

[724] Ibid., 195.

[725] Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action, In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing Data Protection?* (Springer Netherlands, 2009), 3–44. Orla Lynskey, The foundations of EU data protection law, Oxford studies in European law (Oxford University Press, 2015). Paul Bernal, Internet Privacy Rights: Rights to Protect Autonomy (Cambridge University Press, 2014).

[726] J. Bing, A Comparative Outline of Privacy Legislation, Comparative Law Yearbook 1978, vol 2, p. 170.

[727] Anton Vedder, Privacy 3.0. In Van der Hof S., Groothuis M. (eds.) Innovating government: Normative, Policy and Technological Dimensions of Modern Government. (Springer/TMC Asser Press, 2011).

[728] Privacy can be conceptualise in different ways, most importantly as a right 'to be let alone', limited access to the self, secrecy, control over one's personal data, personhood (the ability to develop personal relations and make choices without undue interference), intimacy. See Daniel J. Solove*,* Conceptualizing Privacy*,* 90 Cal. L. Rev. 1087-1155 (2002).

[729] Kristina Irion, Giacomo Luchetta, 'Online personal data processing and the EU data protection reform', Regulatory Policy, CEPS Task Force Reports, 2013, 23.

[730] Bert-Jaap Koops; The trouble with European data protection law. International Data Privacy Law 2014; 4 (4): 250-261. See also Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, Christopher Millard; The language of data privacy law (and how it differs from reality). *International Data Privacy Law* 2016; 6 (4): 259-260 (who claim in relation to the GDPR, that there is "a troubling disconnect between what the rule in question is seeking to achieve and any result it realistically may hope to produce").

[731] Bert-Jaap Koops; The trouble with European data protection law. *International Data Privacy Law* 2014; 4 (4): 250-261.

[732] Christopher Kuner, Fred H. Cate, Christopher Millard, Dan Jerker B. Svantesson, Orla Lynskey; The data protection credibility crisis. *International Data Privacy Law* 2015; 5 (3): 161-162.

data processing into data protection law leads to artificial expansion of its scope and to the "framing [of] Internet-related problems as data protection problems".[733]

The use of risk and reliance on risk assessments as a regulatory tool demonstrates the "ongoing crisis of policy-making". [734] Potential risks and their impact are too complex to be caught by "comprehensive regulatory instruments such as the law or political decision-making processes"[735]. Therefore, *ex ante* focus on enforced self-regulation, and in particular a new obligation on data controllers to conduct Data Protection Impact Assessments (DPIAs), allows for a shift in the responsibility and blame from policy makers to data controllers.

Yet, it is questionable whether the GDPR has "too much faith in controller actions" and they capacity and position to assess risks and prevent unnecessary data processing.[736] Data "controllers do not intend to restrict data processing to the bare minimum" and can easily accommodate their practices into what is 'necessary' for the purposes they define themselves until in rare situations they are checked by the data protection authorities.[737] Also, due to the absence of legislative rules and responsibility on their behalf, data controllers are likely to use "upstream adjudication": anticipate court opinion on a specific risky processing and interferences with the rights and freedoms of data subjects and obligations to use certain procedures, such as stakeholder consultations.[738] The risk-based approach as "the key enforcement method (…) leaving data protection issues mainly to data controllers to decide" is certainly debatable as regards its effectiveness.[739]

5.2. Undefinable and unmeasurable risk as a core element of the shifts

Risk regulation and the risk-based approach first and foremost requires a clear understanding and definition of risk. However, both in theory and in practise privacy risks do not yield an easy definition. Theoretically, risk as a concept can be studied from various disciplines, ranging from philosophy, to natural sciences and economics, and across those different fields acquire diverse connotations.[740] In fact, in the risk literature, the concept of risk can refer to an expected value, a probability or a cause of an unwanted event, which may or may not occur, as much as to the unwanted event or uncertainty as such.[741] Without aiming to provide an exhaustive summary of these definitions, a brief look into the main risk features in several selected fields is provided below.

Natural scientists, in the disciplines such as engineering, toxicology, epidemiology, adopt a rationalist approach to risk and generally treat risk as an objective, measurable

---

[733] Bert-Jaap Koops; The trouble with European data protection law. International Data Privacy Law 2014; 4 (4): 250-261, 258.

[734] L Hempel and H Lammerant, 'Impact Assessments as Negotiated Knowledge' in S Gutwirth, R Leenes, and P De Hert (eds), *Reforming European Data Protection Law* (Springer 2015) 130.

[735] Ibid.

[736] Bert-Jaap Koops; The trouble with European data protection law. International Data Privacy Law 2014; 4 (4): 250-261, 255 ("I fear that, as long as data protection is not in the hearts and minds of data controllers—and the law so far has done a poor job in reaching those hearts and minds […] —mandatory data protection impact assessments will function as paper checklists that controllers duly fill in, tick off, and file away to duly show to auditors or supervisory authorities if they ever ask for it. Procedure followed, problem solved.")

[737] Bert-Jaap Koops, supra note, 254 - 255.

[738] N van Dijk, R Gellert, and K Rommetveit, 'A risk to a right? Beyond data protection risk assessments' 32(2)(2015) Computer Law & Security Review 286, 300.

[739] ME Gonçalves, 'The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward' (2017) 26(2) *Information & Communications Technology Law* 90, 114.

[740] For a detailed review of risk definitions see Ortwin Renn, Concepts of Risk: A Classification. In: S. Krimsky and D. Golding (eds.): Social Theories of Risk. Westport, CT (Praeger 1992), pp. 53-79

[741] Terje Aven, Ortwin Renn, Risk Management and Governance: Concepts, Guidelines and Applications, Series: Risk, Governance and Society, Vol. 16, 2010

phenomenon. They focus on identification of risks, their causes, predictive models of risks and individual responses to risks, or proposals on how to limit the effects of risks. Expert knowledge and scientific calculations dominate in this, so called technico-scientific, approach to risk.[742] The natural science perspective is useful to "anticipate potential physical harm to human being or ecosystems, average these events over time and space, and use relative frequencies (observed or modeled) as a means to specify probabilities"[743].

In contrast to technico-scientific approach, sociologists refer to risk as a socio-cultural phenomenon.[744] Risk is seen as a cultural and social construction undertaken by humans rather as a taken-for-granted objective, material condition, which can be quantified and measured.[745] Despite their nuanced theoretical assumptions of social and cultural theories, and competing positions on risk ranging from a weak social constructionist to relativist, social scientists generally tend to emphasise the broader social, cultural and political context from which risk gains its meaning.[746] The understanding of risk is created through social interpretation and is always linked to group values and interests.[747] Sociologists are therefore less interested in the nature of risk itself, but rather "the forms of knowledge, the dominant discourses and expert techniques and institutions that serve to render risk calculable and knowable, bringing it into being".[748]

Data protection law does not seem to systematically follow one of the above-mentioned understandings of risk. From the inception of the Data Protection Directive the understanding of the concept of risk seems to fit at least in two perspectives: technico-scientific and sociological. Risk first entered the data protection domain as an objective, measurable phenomenon.The *travaux préparatoires* of the Data Protection Directive demonstrate that risk as a term initially was used only in a purely technical, data security-related context. Risk referred to the security measures that were needed in the assessment of the potential security

---

742 Deborah Lupton (ed.), Risk and Sociocultural Theory: New Directions and Perspectives, Cambridge University Press, 2000.

743 Ortwin Renn, Concepts of Risk: A Classification. In: S. Krimsky and D. Golding (eds.): Social Theories of Risk. Westport, CT (Praeger 1992), p. 59

744 Lupton Risk and Sociocultural Theory: New Directions and Perspectives, Cambridge University Press, 2000.

745 Taylor-Gooby & Zin (eds.), Risk in Social Science, Oxford University Press, 2006. Sheldon *Krimsky* and Dominic *Golding (eds.) Social theories of risk*, Westport, CT: Greenwood Publishing Group, 1992. Also on Cultural approach see: M. Douglas and A.B. Wildavsky, *Risk and Culture: An Essay on the Selection of Technical and Environmental Dangers*. Berkeley, 1982, CA: University of California Press. M. Thompson and A. Wildavsky, 'A Proposal to Cerate a Cultural Theory of Risk', 145–161, in H. C. Kunrreuther and E. V. Ley (eds.), *The Risk Analysis Controversy. An Institutional Perspective*. 1982. Berlin: Springer. On system theory see: N. Luhmann, *Risk: a Sociological Theory*. 1993, New York: A. de Gruyter. On Risk Society see: Beck, U. (1992). *Risk Society: Towards a New Modernity.* London, Newbury Park, Calif: Sage Publications. U. Beck, A. Giddens, and S. Lash (eds.), *Reflexive Modernisation: Politics, Tradition and Aesthetics in the Modern Social Order.* Cambridge: Polity Press. On governmentality approach see: Foucault, M. (1991). 'Governmentality', in G. Burchell et al. (eds.), *The Foucault Effect.* London: Harvester Wheatsheaf, pp. 87–104.

746 On a more detailed model of the risk continuum ranging from a realist approach offered in technico-scientific approaches to a highly relativist constructionist approach see Deborah Lupton (ed.), Risk and Sociocultural Theory: New Directions and Perspectives, Cambridge University Press, 1999, Chapter 2. On a taxonomy of sociological approaches to risk see Ortwin Renn, Concepts of Risk: A Classification. In: S. Krimsky and D. Golding (eds.): Social Theories of Risk. Westport, CT (Praeger 1992), pp. 67-72 (Renn orders sociological approaches to risk according to two dimensions: 1) individualistic v. structural; 2) objective versus constructivist. These approaches are: the rational actor concept, social mobilization theory, organizational theory, systems theory, neo-Marxist and critical theory, and social constructionist theory).

747 Ortwin Renn, Concepts of Risk: A Classification. In: S. Krimsky and D. Golding (eds.): Social Theories of Risk. Westport, CT (Praeger 1992), p. 72

748 Deborah Lupton (ed.), Risk and Sociocultural Theory: New Directions and Perspectives, Cambridge University Press, 1999, p. 6

risks.[749] This technical reference to risk is not surprising, considering the fact that the Proposal for the Directive was submitted together with two other highly technical legislative acts: a Directive related to the protection of personal data and privacy in the context of public digital telecommunications network and a Decision concerning the field of information security.[750] Later, more subjective, individual-centered references to risk, i.e. risk as negative impact on a data subject's rights and freedoms, were added after the amendments to the Data Protection Directive proposed by the Parliament. However, in this sense risk as a term was used erratically and equated to danger and threat.[751] The latter terms are used interchangeably with risk in the Commentary attached to the Amended Proposal for a Directive.[752] Yet, risk is conceptually different and should not be conflated with danger.[753]

The debate around the General Data Protection Regulation in the Council once again revealed diverging perception and understanding of risk in the area of personal data protection. It demonstrated a high level of uncertainty among the Member States as to how risk as a term should be understood and categorised. It has been claimed that definition of risk is problematic or non-achievable as: 1) the level of risk is highly context-dependent; 2) it is difficult to arrive at a risk definition that would stand the test of time; 3) law cannot take into account all current risks, but even less regulate future risks, famously called 'unknown unknowns' ('things we don't know that we don't know')[754].

Although risk assessment and measurement were not of a paramount importance before, with the General Data Protection Regulation, which relies on risk in the context of obligations for data controllers, data protection authorities and data controllers will be asked to assess and measure the risks to individuals. The value of risk in quantitative or qualitative terms in the information security area can be objectively defined and established through the undesirable events and threats that make such events possible. Numerous methodologies in this field can help to identify, measure (establish probability and severity), score and mitigate security risks.[755]

The risk evaluation seems to be much more problematic as far as the negative impact on a data subject's rights and freedoms (sociological perspective) is concerned. Some

---

[749] Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990)314—2, 1990/0287/COD ('Initial Proposal').

[750] Proposal for a Council Directive concerning the protection of personal data and privacy in the context of public digital telecommunications networks, in particular the integrated services digital network (ISDN) and public digital mobile networks, COM/90/314FINAL - SYN 288, OJ *C 277, 5.11.1990*; Proposal for a Council Decision in the field of information security, COM/90/314FINAL, *OJ C 277, 5.11.1990.*

[751] For example, commentary on Article 17 'Security of Processing' refers to the 'potential danger to the data subject's right to privacy' emanating from a data controller or a third party (Amended Proposal, 27)

[752] Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Amended Proposal'), COM (92) 422 final—SYN 287, 15 October 1992. It can be accessed on the Archive of European Integration of the University of Pittsburgh <http://aei.pitt.edu/10375>.

[753] Niklas Luhmann (1987) The morality of risk and the risk of morality, International Review of Sociology Series 1, 1:3, 87-101 (notes that risk refers to a possibility of negative effect attributable to one's own decision, danger refers to the possibility of being harmed caused by an external source without individual's choice).

[754] Council of the European Union, 'Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Risk based approach' 12267/2/14 REV 2, 2 September 2014, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2012267%202014%20REV%202> accessed 15 February 2015.

[755] See also e.g. ISO/IEC 27002 security standard 'Information technology – Security techniques – Code of practice for information security management'.

academics have tried to articulate the harms of privacy violations[756], but there is still no consensus around what constitutes such harms and it is hardly possible to develop an exhaustive list of harms resulting from data processing. Regulators and companies have equally failed to identify a comprehensive list of privacy harms and negative impacts on data subjects.[757] It should be mentioned, however, that the Council in the General Data Protection Regulation tried to articulate an indicative list of harms in the context of the DPIA referring to "discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorised reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage" (Article 33.2a). Nonetheless, the list is more illustrative than comprehensive and cannot be easily transferred into operational risk management methodologies. The full understanding of the harms and potential as well as actual negative impacts on individuals is a starting point for the discussion on risk assessment in data protection.

Not less importantly, data driven-technologies and applications can have a negative impact not only to the rights of individuals but also to their groups and the society at large. The GDPR acknowledges the group and societal dimension of privacy risks, but remains unclear about their assessment and measurement in practice. As noted by Spina, "(t)he new digital service and products, in fact, present risks that cannot be easily measured or quantified in accordance with a mere technocratic paradigm; they do not only affect the individuals that use them, but transform the collective fabric of our society; they concern the cognitive rather than the physical integrity of human beings."[758]

However even if better conceptualized, negative impact on individuals (damage) will often be nonphysical and intangible, such as discrimination, reputational and moral damage or any other social disadvantage. Therefore, in practice it will not easily yield to quantification and measurement. Negative impact can also be very subjective, vary from one individual to another or from group to group and cannot be easily known by the data controller. On an individual level, the perception of something as being risky is often based on one's own previous experience, age and understanding. Also, many collective factors, such as education system, cultural values or regulatory framework, may determine that something is being seen as a risk by particular people or nations. For example, as regards children's activities online, their perception of privacy risks, among many other factors, could be shaped by the mediating practises of parents and teachers, influence of school and peers, and individual usage of the Internet.[759] As a result, individuals exposed to the same risks will not experience the same harm. Some will be able to cope with risks while others not. Are the general DPIA frameworks then adequate to fully address the risks to vulnerable data subjects, such as children, or should they be tailored to specific data subjects' needs and vulnerabilities? As the harm is non-physical, and thus hardly measurable, and is subjective (best known to the individuals themselves), it is questionable if the burden for evaluating risks and preventing harm is rightly placed on the data controllers. Can they be expected to foresee and adequately assess all

---

[756] M. Ryan Calo, Essay, *The Boundaries of Privacy Harm*, 86 Ind. L.J. 1131-62 (2011). Lynskey, Orla (2015) The foundations of EU data protection law, Oxford studies in European law (Oxford University Press, 2015), p. 86.

[757] National Institute of Standards and Technology, NIST Privacy Engineering Objectives and Risk Model Discussion Draft (2014), 3. Some efforts to articulate privacy harms, however, include: Centre for Information Policy Leadership at Hunton &Williams LLP, A Risk-based Approach to Privacy: Improving Effectiveness in Practice 2 (2014), see also Centre for Information Policy Leadership at Hunton &Williams LLP, The Role of Risk Management in Data Protection (2014).

[758] A. Spina (2017). A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics. European Journal of Risk Regulation, 8(1), 88-94, at 89-90.

[759] Ellen J Helsper, et al, "Country Classification: Opportunities, Risks, Harm and Parental Mediation" (2013) LSE-EU Kids Online, available at <http://eprints.lse.ac.uk/52023/> accessed 30 August 2017

potential negative impacts (harm) on individuals of their proposed data uses and device appropriate protection measures?[760] How to guarantee that their assessments ensure an even level of protection across the EU when there are different risk assessment methodologies used?[761] How can data controllers be liable for the methodological choices and subjective risk perceptions?[762] These questions underline the challenges that the reliance on risks and risk management in data protection has brought, that require further guidance and clarification from the EDPB and the courts. In the meantime, if risk to individuals cannot be adequately defined and evaluated, the shift towards risk regulation can lead to lowering the data protection level from the perspective of the data subjects. As noted by Lynskey, a concern exists that 'data controllers, processors, and DPAs will underestimate the risks entailed by certain personal data processing, leading to an under-enforcement of rules'[763].

The General Data Protection Regulation heavily relies on risk management through Data Protection Impact Assessments. In order to manage privacy risks, they have to be simplified, operationalized and measured according to a chosen methodology. Given the ambiguous nature of risk as a concept, uncertainty and limited knowledge of risks, risk assessment techniques have been criticised due to the lack of objectivity, the unclear methodological assumptions and choices and the limits of scientific knowledge.[764] As Power notes too much manageability of risks according to 'well tried, incrementally adjusted, linear frameworks of understanding' can lead to a pretence of control and rather than effective mechanisms.[765] Thus, when risks are integrated into formalised risk management frameworks, they may lose substance and meaning.[766]

Existing privacy risk management methodologies and guidelines try to express data protection concepts and principles in risk management terminology, but face epistemic challenges.[767] For example, in the CNIL's methodology, risk means a 'scenario describing a feared event and all threats that make it possible'.[768] Thus, risk is expressed through two measurable components: undesirable events (what do we fear?) and threats (how can this

---

[760] De Hert and Papakonstantinou state "great expectations for data controllers' responsible behaviour are made" in the GDPR requiring to conduct DPIA and "It remains therefore to be seen whether the positive example of environmental and other impact assessments will be repeated in the data protection field as well". Paul De Hert, Vagelis Papakonstantinou, The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals, Computer Law & Security Review, 28(2), 2012, Pages 130–142, p. 141.

[761] Raphaël Gellert, Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative, *International Data Privacy Law (2015) 5 (1): 3-19.*

[762] Ibid.

[763] Lynskey, Orla (2015) The foundations of EU data protection law, Oxford studies in European law (Oxford University Press, 2015), p. 86.

[764] See Paul Harremoës and others (eds), *The Precautionary Principle in the 20th Century: Late Lessons from Early Warnings* (Earthscan, London; Sterling, VA 2002), p. 22.

[765] Michael Power, *The Risk Management of Everything—Rethinking the Politics of Uncertainty* (Demos, London 2004), p. 19

[766] Raphaël Gellert, Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative, *International Data Privacy Law (2015) 5 (1): 3-19, 16.*

[767] Ibid, 16-17. See also Stuart S. Shapiro, "Situating Anonymization Within a Privacy Risk Model," Homeland Security Systems Engineering and Development Institute (2012) at p. 2, available at https://www.mitre.org/sites/default/files/pdf/12_0353.pdf.
who claims that similarly in the US the Fair Information Practice Principles "encourage framing of privacy harms purely in terms of principle violations, as opposed to the actual impact on individuals."

[768] Commission Nationale de l'Informatique et des Libertés (CNIL), 'Methodology for Privacy Risk Management (2012) <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf> accessed 15 February 2015 Commission Nationale de l'Informatique et des Libertés (CNIL), 'Measures for the privacy risk treatment' (2012) A Catalogue of good practices, <http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Measures.pdf> accessed 15 February 2015

occur?), both evaluated in terms of probability and severity according to the scale of 'negligible, limited, significant or maximum' risks.[769] Feared events (e.g. unavailability of legal processes, excessive or unfair data collection, illegitimate access to personal data) are essentially violations of the data protection principles. The majority of threats through which risks may happen are framed in data security terms. They involve function creep, espionage, exceeded limits of operation or damage of supporting assets, property losses. Although this methodology is highly operational and provides a formalised risk management tool, its validity and effectiveness are limited. It fails not only to take into account all the possible threats but also more generally, does not provide much insight regarding the level of data protection within an organisation[770] or indeed adequately consider the actual impact on individuals.

The epistemic problem outlined above is expected to be applicable to other privacy risk management tools and methodologies. While managing privacy risks, they can easily be reduced to void and meaningless statistical expressions of probabilities, focusing on process rather than on content.

VI. Conclusion

European data protection law is in a progressive "riskification" process as manifested in a two-fold shift. Through the implementation of the risk-based approach in the General Data Protection Regulation (the first shift), risk is assigned new functional roles and shapes the regulation. Rooted in data and information security in the Directive 95/46/EC, the new functions of risk expand in constructing the core of the accountability principle, and triggering new obligations for data controllers.

EU data protection law also comes closer to risk regulation (the second shift). It has been demonstrated that the General Data Protection Regulation increasingly reflects the main features that risk regulation, such as regulation of human safety, health or environmental risks, has. Severity and probability are inserted into the General Data Protection Regulation as important risk measurement elements. Risk assessment may be expected to be defined by a specialised, independent, knowledge-based entity the European Data Protection Board - partially denoting a shift toward independent, scientific risk assessment in data protection. There is an effort to hear the views of the data subjects and their representatives on intended data processing operations, and thus let them participate in defining risks and deciding on their management in personal data protection law.

The two shifts present an (unresolved) challenge with the nature of an individual fundamental right of data protection. Fundamental rights regulation, is built on different foundations than risk regulation and the possibility to align them presents complex questions. The use of risk and reliance on risk assessments as a regulatory tool partially shifts the responsibility for the protection of fundamental rights and the blame from policy makers to data controllers. Yet, data controllers are not necessarily in a position to assess risks and prevent unnecessary data processing.

The two shifts are based on an undefined and multidimensional notion of risk, which is not only an obstacle to successfully assess and measure risks, but also might lower the protection level for individuals. In data security, risk is an objective phenomenon, which can be expressed and quantified through feared events and threats. Privacy risks are more subjective and 'individualised', and thus hard to establish, evaluate, and quantify. No uniform understanding of the privacy harms and negative impacts on individuals exists, and privacy risks are too complex to be fully caught by privacy risk management tools and methodologies.

---

[769] Methodology for Privacy Risk Management (supra note) 6.

[770] Raphaël Gellert, Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative, *International Data Privacy Law (2015) 5 (1): 3-19,* 17.

However, the GDPR envisions data protection impact assessments as a key tool that data controllers should rely upon when controlling risks. Indeed, DPIAs will be a mandatory requirement from May 2018. Some of the unresolved challenges, mentioned above, could be addressed through the development of sector-specific or technology-specific DPIA frameworks or codes of practice, allowing for the development of methodologies specialized for specific application contexts or architectures. Frameworks for a specific type of data subjects, such as children, the elderly and others groups of individuals requiring special protection, could also be considered as they could address the particular needs and rights of these data subjects. In conclusion, therefore such focused analysis of particular risks requires further research and specification.

Chapter 6

Constructing Child-Specific Privacy Impact Assessments

Presented at the 2nd European edition of the Privacy Law Scholars Conference (PLSC-Europe), 19 May 2017, at Tilburg University.

Submitted to a peer-reviewed journal as:

Milda Macenaite, Sourya Joyee De, Daniel Le Métayer, Constructing Child Specific Privacy Impact Assessments.

Abstract

From 25 May 2018, data protection impact assessments (DPIAs) will become a key tool that data controllers should rely upon when controlling high risk to the rights and freedoms of individuals. Given the need to tailor DPIAs to specific technologies, sectors, and data subjects, the paper provides guidelines to facilitate the achievement of the child-specific DPIA. Based on the PRIAM methodology, the paper discusses technical aspects of the child-tailored DPIA specifying its concrete component (personal data, risk sources, feared events, privacy weaknesses and privacy harms) and their attributes, and provides examples related to risks for children in the information society context. The proposed framework enables data controller to address the particular needs and rights of children as data subjects.

Key words:

data protection impact assessment, children, child rights, General Data Protection Regulation,

1. Introduction

The EU General Data Protection Regulation 2016/679 (GDPR)[771] envisions data protection impact assessments as a key tool that data controllers should rely upon when controlling high risk to the rights and freedoms of individuals. DPIAs will be a mandatory requirement from 25 May 2018. This new requirement aims to shift data protection from paper-based bureaucratic requirements towards compliance in practice[772] and enhance accountability, transparency, as well as potentially foster the data protection culture and responsibility *vis-à-vis* data subjects among data controllers. Beyond this legal requirement, conducting a DPIA is a recommended step for any company intending to develop and operate a system or a service that processes personal data. Technological developments that are developed too hastily without the assessment of risk can have a negative impact on individuals, thus leading to

[771] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[772] Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) 11 Privacy & Security Law Report, 6, p. 1.

considerable damage to the company's reputation and potentially triggering strong public opposition.[773]

The GDPR provides general criteria that have to be met by DPIA methodologies. The DPIA is envisioned as being carried out from data subjects', rather than from data controllers', perspective in order to actually to take into account risks to the rights and freedoms of individuals.[774] Therefore, not only the development of sector-specific or technology-specific DPIA frameworks, specialized for specific application contexts or architectures, should be encouraged, but also frameworks for a specific type of data subjects, such as children, the elderly and others groups of individuals requiring special protection. These data subject-tailored DPIAs could address the particular needs and rights of specific data subjects.

The GDPR explicitly recognises that children deserve special protection as data subjects (Recital 38), especially online, and specific safeguards and protections should apply to children's personal data. The importance to consider the status of the data subject, e.g. if the data subject is a child or otherwise belongs to a more vulnerable segment of the population, when assessing the impact of data processing operations has been underlined by the Article 29 Working Party on several occasions.[775] In the same vein, in the context of personal data protection online, the European Data Protection Supervisor (EDPS) has acknowledged that data protection and privacy risks to children 'must be addressed in a manner appropriate to the specificity and vulnerability of the category of individuals at risk'[776]. Assessing risks to children and other vulnerable members of the population is already a frequent practice in other risk regulation areas, such as in the EU chemicals regulation.[777] As a consequence, when children's personal data is collected and processed, data controllers should consider carrying out a child-specific DPIA. With this in mind, the paper proposes a way to adapt the general GDPR requirements for the DPIA to cases when data subjects are children and illustrates how a child-specific DPIA could be carried out based on the PRIAM methodology. The paper particularly focuses on personal data processing online and provides examples related to risks for children in the information society context.

This paper is divided in five parts. The second part identifies the reasons for carrying child-specific DPIAs when processing children's personal data in the online world. The third part lists the general GDPR criteria for the DPIA content. In the fourth part, the specific risk

---

[773] Public campaign by the child development and privacy experts and thousands of parents against Aristotle, an IoT system for children, developed by Mattel, Inc. due to privacy and child development concerns. See Letter to Mattel, 2 October 2017, http://www.commercialfreechildhood.org/sites/default/files/Letter%20to%20Mattel.pdf. As a result, the product has been cancelled before its release. See Hayley Tsukayama, Mattel has cancelled plans for a kid-focused AI device that drew privacy concerns, 4 October 2017, available at: https://www.washingtonpost.com/news/the-switch/wp/2017/10/04/mattel-has-an-ai-device-to-soothe-babies-experts-are-begging-them-not-to-sell-it/?utm_term=.14c79beeb1be
Public campaign by child advocacy, consumer and privacy groups against "smartwatches" that allow the monitoring of young children due to major security and privacy problems, Letter to the Federal Trade Commission, available at: 18 October 2017, available at: http://www.commercialfreechildhood.org/sites/default/files/Smart%20Watch%20FTC%20letter%2010.18%20FINAL.pdf , Campaign for a Commercial-Free Childhood, Stop Mattel's "Hello Barbie" Eavesdropping Doll, (Feb. 2015) http://www.commercialfreechildhood.org/action/shut-down-hello-barbie

[774] Christopher Kuner, 'The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law' (2012) 11 Privacy & Security Law Report, 6

[775] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, WP 217 ; Opinion 03/2013 on purpose limitation, 2 April 2013, WP 203.

[776] EDPS, Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", 17 July 2012.

[777] Kristina Nordlander, Carl-Michael Simon and Hazel Pearson, 'Hazard v. Risk in EU Chemicals Regulation' (2010) *European Journal of Risk Regulation 3,* 239-250, 241.

management methodology (PRIAM) chosen for this paper is presented. The fifth part adapts PRIAM risk management methodology focusing on its criteria (personal data, risk sources, feared events, privacy weaknesses and privacy harms) and attributes for the proposed child-specific DPIA framework. Conclusions are drawn in the last part.

2. Why child-specific DPIAs?

The GDPR data protection impact assessment process is generic and does not address specifically the risks to children as data subjects. The lack of adaptation of the DPIA framework to children as data subjects when assessing risks to their rights and freedoms resulting from data processing operations presents several problems. First, the general DPIA framework is not able to take into account the specific characteristics of children as data subjects and consumers, i.e. specific developmental features (vulnerabilities, needs) and the different behaviour of children. For example, due to their particular behavioural characteristics, such as emotional volatility and impulsiveness, children (especially teenagers) are seen as being vulnerable in comparison to adults online[778]: more active and risk-prone,[779] less capable of evaluating perilous situations, given their lack of awareness vis-à-vis the long-term consequences of their virtual actions.[780] The data controllers should take into account these specific developmental features and make sure that they are not exploited in their services and data collection practices. Concerns have been raised, for example, about special techniques employed by companies towards children, such as "real-time bidding, location targeting (especially when the user is near a point of purchase), and "dynamic creative" ads tailored to their individual profile and behavioral patterns"[781]. Unfair commercial practices, in particular emotional manipulation based on profiling in online services, aggressive and immersive marketing and advertising, have been criticised as having negative impact on children's rights and wellbeing.[782]

Second, the risk factors should be considered in a different way for children than for adult data subjects due to the different inputs, or parameters, of the risk analysis. In case of children, potential negative impacts (harm) can be more serious or damaging and there might (often) be a higher probability of such an impact occurring.

---

[778] Judith Bessant, 'Hard wired for risk: neurological science, 'the adolescent brain' and developmental theory', (2008) 11(3) Journal of Youth Studies 347, 358 (criticises research on adolescent brain as "it begins with a prejudice ('they' are 'different' 'irrational' and 'deficient') and then threatens to expand the civil and social disadvantages that already severely affect too many of our young people". Bessant claims that "some young people are sometimes at risk not because their brains are different, but because they have not had the experience or opportunity to develop the skills and judgment that engagement in those activities and experiences supply".)

[779] Andrew Hope, 'Risk-taking, boundary-performance and intentional school internet 'misuse'', (2007) 28(1) Discourse: studies in the cultural politics of education 87.

[780] Jay N Giedd, 'The Teen Brain: Insights from neuroimaging', (2008) 42(4) Journal of Adolescent Health 335; Elizabeth R McAnarney, 'Adolescent Brain Development: Forging New Links?' (2008) 42(4) Journal of Adolescent Health 321; Tim McCreanor et al. 'Consuming identities: Alcohol marketing and the commodification of youth experience', (2009) 13 (6) Addiction Research & Theory 579; Laurence Steinberg, 'Risk taking in adolescence: New perspectives from brain and behavioral science', (2007) 16 (2) Current Directions in Psychological Science 55; Laurence Steinberg, 'Social neuroscience perspective on adolescent risk-taking' (2008) 28(1) Developmental Review 78.

[781] Kathryn C. Montgomery, 'Youth and surveillance in the Facebook era', (2015) 39(9) Telecommunications Policy 771; Kathryn C Montgomery and Jeff Chester, 'Data protection for youth in the digital age: Developing a rights -based global framework', (2015)1(4) European Data Protection Law Review 291.

[782] European NGO Alliance for Child Safety Online (eNACSO) (2016) *When Free Isn't: Business, Children and the Internet*. Rome: eNACSO. Available at: www.enacso.eu/wp-content/uploads/2015/12/free-isnt.pdf; Verdoodt, V., Clifford, D., Lievens, E. (2016), Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU, 32 Computer Law & Security Review 599

Third, a specific catalogue of fundamental rights and freedoms should be taken into account by child-oriented product and service providers in DPIAs. The Article 29 Working Party stressed that the GDPR refers to risks posed not only to the rights to privacy and personal data protection, but also to other human rights and freedoms, such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.[783] Children are entitled to more elaborate catalogue of internationally recognised fundamental rights compared to adults as established by the UN Convention on the Rights of the Child (UN CRC). Some UN CRC principles, such as the best interest of the child principle and the right to be heard, and some rights, such as the protection from harmful information or the right to play, are uniquely granted to children and not to adults by international law. As shown in Table 1, the child rights enshrined in the UN CRC can be divided into general principles, i.e. fundamental values to be considered when interpreting and implementing all the other child rights, and three right categories: protection, provision and participation rights. These distinctions are useful as far as they clearly convey the primary aim of the specific child rights but are not clear-cut as, according to the general principles of the UN CRC, all rights should incorporate a participation, provision and protection component.[784] In other words, even if the right to privacy traditionally falls under the protection category[785], its provision and participation aspects are equally important.[786]

Although the UN CRC, as an instrument, is applicable to the states and does not directly impose positive obligations to the same extent on the companies, data controllers are obliged to respect child rights. EU law is interpreted in light of the constitutional traditions of the Member States and public international law. As the UN CRC is public international law which the EU Member States all have incorporated as part of their national regimes and constitutional traditions it is necessary to assume that laws need to be interpreted with the children's rights framework in mind.

Another reason why businesses should respect and support children's rights stems from their corporate social responsibility and the global standards, such as UN Guiding Principles on Business and Human Rights[787], the Children's Rights and Business Principles[788] and Guidelines for Industry on Child Online Protection[789]. According to the UN Guiding Principles on Business and Human Rights, the responsibility of business to respect human rights means: 1) "avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur"; and 2) "seek to prevent or mitigate adverse human

---

[783] Article 29 Data Protection Working Party, 'Statement on the Role of a Risk-based Approach in Data Protection Legal Frameworks', WP 218, 30 May 2014.

[784] Eugeen Verhellen, 'The Convention on the Rights of the Child: reflections from a historical, social policy and educational perspective' in Wouter Vandenhole, Ellen Desmet, Didier Reynaert, Sara Lembrechts (eds.) Routledge International Handbook of Children's Rights Studies, 2015.

[785] For a possible categorization of child rights see e.g. Sonia Livingstone, Children's digital rights: a priority. Intermedia, 2014, 42 (4/5).

[786] In the context of privacy, it could be argued that children's participatory rights should be brought to the forefront and used to inform all of the issues listed in Table 1 in order to counter the protective bias within the GDPR and more fully actualize the promise of agency within the UN CRC. On the protective bias and the GDPR see Macenaite M., From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation, 19(5) New Media & Society, 2017, pp. 765 - 779.

[787] UN, Guiding Principles on Business and Human Rights, 2011, available at: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

[788] UNICEF, the UN Global Compact and Save the Children, Children's Rights and Business Principles, 2013, at:https://www.unglobalcompact.org/docs/issues_doc/human_rights/CRBP/Childrens_Rights_and_Business_Principles.pdf

[789] International Telecommunication Union (ITU) and the United Nations Children's Fund (UNICEF), Guidelines for Industry on Child Online Protection, 2015, at: https://www.unicef.org/csr/files/COP_Guidelines_English.pdf

rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts".[790]

Therefore, when assessing the risks to the rights and freedoms of individuals, in addition to the age-generic human rights, data controllers should carefully consider children's rights and the general principles enshrined in the UN CRC. Moreover, it is not only the impact on relevant rights that has to be assessed but also the balance between the rights should be taken into account. For example, a balance must be struck between participation and protection rights, that reflects a particular child's age and maturity. In this respect, it has been noted that "a rights framework provides a normative lens through which to critically examine and evaluate the benefits or harms of children's growing access to and provision of digital technologies"[791]. Indeed, for example one should avoid discussing "protection challenges without recognising how the resulting policy can curtail children's freedoms to participate online".[792]

Table 1: UN CRC child rights catalogue relevant for the child-specific DPIAs

Categories	**UN CRC provision**	**Examples of relevant risks and issues online**
General Principles	Art. 2: the right to non-discrimination	Profiling and data mining resulting in discriminatory decisions, discrimination in accessing online services
	Art. 3: the best interest of the child principle – 'in all actions concerning children (...) the best interests of the child shall be a primary consideration'	Services and products that are directed to children and are designed without considering the best interest of the child principle, e.g. a location tracking device meant for children not having adequate data security measures leading to the leak of the location of the child to people other than parents.
	Art. 6: Right to life, survival and development:	Services and products do not allow the development of the child's personality, talents and mental and physical abilities to their fullest potential.
	Art. 12: the right to be heard - the right	Overprotective parental consent mechanisms not

[790] UN, Guiding Principles on Business and Human Rights, 2011, at: http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf, p. 14.
[791] Mariya Stoilova, Livingstone, S. and Kardefelt-Winther, Global Kids Online: Researching children's rights in a global digital age, *Global Studies of Childhood*, 2016 6(4), 455-466, 456.
[792] Ibid.

	of children (capable of forming their own views) to be consulted in all matters affecting them and being given due weight in accordance with the age and maturity	allowing to consult children, DPIAs carried out without consulting children as stakeholders
Protection, provision and participation rights	Art. 19: Protection against all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation	Cyberbullying, harassment, embarrassment, humiliation, defamation.
	Art. 34: Protection from sexual exploitation and sexual abuse	Grooming, sexual exploitation, inappropriate notice and takedown procedures of child sexual abuse material
	Art. 36: Protection from 'all other forms of exploitation prejudicial to any aspects of the child's welfare'	Unfair commercial practices (e.g. emotional manipulation in online services, aggressive and immersive marketing and advertising), inadequate children's data security and protection measures
	Art. 17(e): Protection of the child from 'information and material injurious to his or her well-being'	Unlimited exposure to (extreme and illegal) pornography or violence
	Article 16: Protection from 'arbitrary or unlawful interference with (…) privacy, family, or correspondence', unlawful attacks on child's honour and reputation'	Unlawful and unfair personal data processing (e.g. invalid consent, inadequate and unclear information disclosure, ineffective data subject rights), personal data misuse, excessive parental monitoring, filtering and tracking of online activities.
	Art. 8: the right of the child to preserve his or her identity	Online impersonation, profile hacking, ineffective right to erasure
	Art. 31: Provision and support of children's rights to 'rest and leisure, to engage in play and recreational activities appropriate to the age'	Lack of age-verification in child-inappropriate online services
	Art. 28 and 29: provision of an education that will support the development of child's full potential and prepare them 'for responsible life in a free society'	Unavailability of educational online services and features, lack of online safety information and awareness raising

	Art. 17: provision 'access to information and material from a diversity of national and international sources, especially those aimed at the promotion of (…) social, spiritual and moral well-being and physical and mental health	'Filter bubble' and selective information availability, news personalisation
	Art. 13: the child's right to freedom of expression (including 'freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice')	Unjustified or disproportionate limitations of online connections, access to virtual communities and social networking websites.
	Art. 15: the child's right to freedom of association and peaceful assembly.	Limited networking opportunities, restrictions to associate with others for social, political or cultural purposes

Adapted from Sonia Livingstone (2014) Children's digital rights: a priority. Intermedia, 42 (4/5). 20-24; UK Children's Commissioner, 'Growing Up Digital: A report of the Growing Up Digital Taskforce' (January 2017)

3. GDPR requirements for the data protection impact assessments

The need to account for new risks to individuals created by technological, in particular data-driven, advances and developments has led to the introduction of a new enforced self-regulatory tool, the DPIA, in data protection law. Under certain conditions, the DPIA has become a new obligation for data controllers in Europe requiring to manage risks to the rights and freedoms of data subjects through three interconnected processes: context description (the nature, scope, context and purposes of data processing, the sources of the risk), risk assessment, and risk mitigation.[793]

In line with the risk-based approach followed by the GDPR, the DPIA is not always required, but only when data processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1)). Some of the examples, illustrated by Article 35(3), include automated data processing for the purpose of profiling intended to evaluate personal aspects of individuals that create legal effects or have a significant impact, processing of special data categories such as health data on a large scale and a systematic monitoring of public areas on a large scale. Although neither the GDPR in Article 35(3)[794] nor the Article 29 Working

[793] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4 April 2017.

[794] The initial GDPR proposal published by the European Commission on 25 January 2012 included children's data among the data categories for which the DPIA was required. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final, 25 January 2012.

Party in its recent guidelines[795] explicitly ask for a mandatory DPIA for all the systems involving personal data about children, it acknowledges that the processing of data belonging to vulnerable data subjects could require a DPIA. The main reason for this is "the increased power imbalance between the data subject and the data controller, meaning the individual may be unable to consent to, or oppose, the processing of his or her data".[796] In particular, "children can be considered as not able to knowingly and thoughtfully oppose or consent to the processing of their data".[797] Also, given the fact that the GDPR establishes a non-exhaustive list of "high risk" data processing operations that are subject to the DPIA requirement, national data protection authorities might include children's data into their lists of data processing operations under the DPIA obligation (Article 35.4). In addition, the Article 29 Working Party advices to carry out a DPIA in situations when it is not entirely clear if it is necessary according to the GDPR, as a DPIA is a useful tool to ensure GDPR compliance.[798] Thus, in many cases, the DPIA will need to be conducted when personal data about children is collected, especially before the creation and deployment of a new product or service.

A DPIA is not formally defined in the GDPR but, according to the Article 29 Working Party, it is "a process designed to describe the processing, assess the necessity and proportionality of a processing and to help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data"[799]. The requirements for its content listed in the GDPR (Article 35(7), and recitals 84, 90) include: 1) a description of the processing operations and their purposes, 2) the assessment of the necessity and proportionality of data processing, 3) the assessment of the risks to the rights and freedoms of data subjects and 4) the measures foreseen to address the risks. These requirements can be met by different DPIA methodologies.

4. Child-specific data protection impact assessments

A number of data protection impact assessment and privacy impact assessment (hereinafter jointly referred to as (D)PIAs) frameworks exists. For example, D. Wright proposes a sixteen-step optimized PIA process based on a review of various existing PIA methodologies.[800] Official bodies such as the CNIL, the ICO, and the Spanish data protection authority have published their (D)PIA guidelines.[801] The Article 29 Working Party (A29WP)

[795] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4 April 2017.
[796] Ibid.
[797] Ibid.
[798] Ibid.
[799] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4 April 2017, p. 4.
[800] David Wright. Making privacy impact assessment more effective. The Information Society, 29(5):307–315, 2013.
[801] Information Commissioner's Office, 'Conducting Privacy Impact Assessments' (2014) Code of Practise, available at: http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/data_protection/practical_application/pia-code-of-practice-final-draft.pdf; Agencia Espanola de Proteccion de Datos, 'Guía para una Evaluación del Impacto en la Protección de Datos Personales' (2014) available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf. Commission Nationale de l'Informatique et des Libertés (CNIL), Privacy Impact Assessment (PIA) Methodology (how to carry out a PIA), (2015) available at: https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

has recently adopted its own guidelines on DPIA[802]. In addition, several (D)PIAs for specific products have been published.[803] All these contributions are very useful to establish the general framework and to help the experts to conduct complex tasks such as deciding whether a full PIA is required or not, organizing the overall process (including planning, stakeholders consultation, resource allocation, audits, etc.) and the main analysis phases (definition of the stakeholders, sources of risk, privacy threats, etc.). However, the majority of them do not define very precisely how the technical part on risks analysis of the privacy risk assessment should be performed.

In contrast, the PRIAM framework[804] chosen as a methodology for this paper, precisely fills this gap and proposes a DPIA methodology which is both rigorous and systematic. It provides all the information required for the risk assessment process and indicates how they can be gathered by clearly listing various attribute-attribute, attribute-category and category-category links. It also takes into account the influence of external factors such as social or legal norms in determining certain categories and attributes. For example, it demonstrates that different attributes of data such as form, retention, sensitivity, volume, etc. along with attributes of other components such as the system[805] can help to determine categories of privacy weaknesses and feared events. Such links are not well-established or, at least, not well-depicted in other DPIA methodologies. PRIAM also allows to connect privacy weaknesses and risk sources to harms via feared events through harm trees.

The PRIAM framework relies on seven components (system, stakeholders, data, risk sources, feared events, harms and privacy weaknesses)[806], the last five are further discussed in the paper. The paper does not present or discuss in detail all the steps and aspects of the PRIAM methodology, but focuses on the main categories and attributes of components which have to be dealt with in a specific way for children. For example, the representation of the system (e.g. based on data flow graphs) is not discussed as it is not affected by the fact that the analysis applies to children.

In a nutshell, risk sources can exploit privacy weaknesses of the system to bring about feared events leading to privacy harms. The methodology consists of two main phases: information gathering and risk assessment based on harm trees. The output of the second phase is the risk level of a harm, expressed as the pair of severity and likelihood. The PRIAM framework includes, for each component:

---

[802] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.

[803] Privacy Impact Assessment for RFID Applications, 2011, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf. Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, 2014, available at: https://ec.europa.eu/energy/sites/ener/files/documents/2014-dpia-smart-grids-forces.pdf.

[804] Sourya Joyee De, Daniel Le Métayer, PRIAM: A Privacy Risk Analysis Methodology (PRIAM Report), RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes, 2016, available at: hal-01302541; Privacy Risk Management for Federal Information Systems, 2015, available at: http://csrc.nist.gov/publications/drafts/nistir-8062/nistir-8062-draft.pdf

[805] The system encompasses the entire life-cycle of the personal data for the application (or set of applications) considered. It consists of various hardware and software components, e.g. the functional specification describing the services that it provides, the interface, the data flows, the supporting assets (e.g., hardware, applications, data stores, software), the actors having access to the system or interacting with it, the controls consisting of legal measures (e.g., contracts between data controllers and third parties) and technical measures (e.g., anonymization techniques, encryption schemes). See Sourya Joyee De, Daniel Le Métayer, PRIAM: A Privacy Risk Analysis Methodology (PRIAM Report), RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes, 2016.

[806] Sourya Joyee De, Daniel Le Métayer, PRIAM: A Privacy Risk Analysis Methodology (PRIAM Report), RR-8876, Inria - Research Centre Grenoble – Rhône-Alpes, 2016.

- a set of categories from which the relevant elements have to be chosen for a given system and
- a set of attributes which have to be defined and used for the computation of the risks.

The categories are useful to find all the relevant input information for the analysis of a given system. For example, data categories include, among others, health data, location data, financial data and contact data; stakeholder categories include data subjects, data controllers, data processors and third parties. The attributes of a component refer to the aspects of the component that can have an effect on privacy risks. For example, the precision level and the retention delay of the personal data collected by a system can affect the likelihood of a privacy risk. The value assigned to an attribute can be either qualitative (e.g., using a fixed scale such as {low, medium, high} or quantitative.

The final output of a risk analysis consists of a list of potential harms with the risk level of a harm being presented as the pair of severity and likelihood. In PRIAM, the likelihood of a harm can be evaluated using harm trees, which is a convenient way to represent the relationship among the exploitation of privacy weaknesses by the risk sources, the feared events and the privacy harms and to assess their probabilities. In a nutshell, the root node of a harm tree denotes a harm. Leaf nodes represent privacy weaknesses exploited by the risk source for the particular harm. Intermediate nodes represent feared events. The tree is structured in branches leading to the harm. Child nodes are connected by an AND node if all of them are necessary to lead to the parent node and OR node if any one of them is enough to lead to the parent node.

PRIAM is a very general methodology which has been applied to various case studies such as smart grids, quantified self and biometric access control systems. As shown by Sourya De and Le Metayer[807], the methodology can also be specialized for specific application contexts or architectures. An interesting question, which is the focus of this paper, is its specialization for a specific type of data subjects, namely children in order to address their needs and rights presented earlier.

5. Components and attributes of child-specific data protection impact assessments

In the next sections, the paper will focus on the main components of the child-specific DPIAs (personal data, risk sources, feared events, privacy weaknesses and privacy harms) and their attributes drawing on the PRIAM methodology.

5.1. Personal Data

The personal data involved in the processing is one of the key components of a DPIA. Personal data, in this paper, refers to any information relating to an identified or identifiable natural person and any information allowing such a person to be singled out or treated differently.[808] The particular types of personal data processed by the system are defined by its functional specification. Social networking sites, for example, according to the taxonomy proposed by C. Richthammer et al., collect the following 13 data categories: login data,

[807] Sourya De, Daniel Le Metayer. A Risk-based Approach to Privacy by Design (Extended Version), Research Report, RR-9001, Inria - Research Centre Grenoble – Rhˆone-Alpes, 2016, available at: hal-01420954.

[808] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] *OJ L 281/0031.*

connection data, application data, mandatory and extended profile data, ratings/interests, network data, contextual data, private communication data, disclosed data, entrusted data, incidental data, disseminated data.[809]

In the following, we first discuss the categories of personal data that are especially relevant for children (Section 5.1.1) before presenting the relevant attributes (Section 5.1.2).

5.1.1. Categories of Personal Data

Although all personal data related to children merit enhanced protection, some particular types of data collected by all information society service providers (regardless of the concrete application or system) can cause higher risks to children than others and their impact should be carefully assessed. For example, IT applications and products that collect and process children's contact information, identification data, biometric data, geolocation, or data related to children's behavior/habits require special attention.[810] Equally, stringent protection measures should be envisioned when IT products and applications are designed to allow the public disclosure of personal data or sharing it with third parties (discussed below).

5.1.1.1. Contact and identification data

Contact information constitute data that permit direct contact with a user online and include his or her phone number, physical address, email address, instant messaging user identifiers, voice over internet protocol identifiers, internet chat user identifiers, and other identifiers, e.g. persistent identifiers that allow users to be recognized and tracked for advertising and other purposes across various online services and websites. Unauthorized access and misuse of contact information and identification data of children may lead not only to minor psychological harms (e.g. undesirable commercial advertising) but also to physical (safety) harms, ranging from cyber or physical bullying, stalking, grooming or other types of physical aggression or sexual exploitation. For example, a child may be groomed and sexually exploited when a paedophile uses his contact or location data.

5.1.1.2. Biometric data

Biometric data (biological properties, behavioural and physiological characteristics, living traits) are unique to a certain individual and measurable.[811] They create a direct link between a human body and his identity due to the translation of human body traits into a machine-readable form.[812] Raw biometric data, e.g. images of children contained in photos,

---

[809] C. Richthammer, M. Netter, M. Riesner and G. Pernul, "Taxonomy for Social Network Data Types from the Viewpoint of Privacy and User Control," *2013 International Conference on Availability, Reliability and Security*, Regensburg, 2013, pp. 141-150.

[810] The Children's Online Privacy Protection Act (COPPA) in the US is one of the few examples of the laws which specifically focus on the protection of children's privacy online. COPPA, for example, protects the following categories of personal information of children: first and last name; a home or other physical address including street name and name of a city or town; online contact information; a screen or user name that functions as online contact information; a telephone number; a social security number; a persistent identifier that can be used to recognize a user over time and across different websites or online services; a photograph, video, or audio file, where such file contains a child's image or voice; geolocation information sufficient to identify street name and name of a city or town; or information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier mentioned above.

[811] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 27 April 2012, WP 193.

[812] Ibid.

videos, and audio files can convey a large amount of personal information about a child, such as information about health, race, ethnic origin, religion or political views (e.g. when wearing religious or political outfits or symbols) and thus images and videos can be considered sensitive data. For example, the Vividown case in Italy demonstrated that a video posted in Google Videos about a disabled child who was bullied and insulted by his classmates, contained sensitive data revealing the child's health condition (autism).[813] However, it would be impractical to subject all images from which religion or ethnicity can be inferred with various degrees of certainty, to stringent data protection requirements applicable to sensitive data. It is therefore acknowledged that images of individuals on the internet do not contain sensitive personal data *"*unless the images are clearly used to reveal sensitive data about individuals."[814,815]

Processing, especially disclosure, of images and videos related to children potentially can put their personal safety at risk. Images and videos can also contain embedded geolocation data. The use of facial and voice recognition technologies, makes images identifiable thus permitting the establishment of physical or online contact with a specific individual".[816] Examples of such technologies used by children and generating complaints from privacy advocates include a facial recognition software used by Facebook to suggest tags and its new facial recognition app "Moments" and voice recognition deployed by the Genesis Toys in their "smart" toys - the My Friend Cayla doll and the i-Que Intelligent Robot.[817]

In addition, some biometric data reveals physical information about a child. This information can be used for profiling, predicting behaviour or preferences and taking automated decisions and lead to discrimination, stigmatization or unwanted confrontation with unexpected or undesirable information.[818]

Employment of biometric technologies for identification and access control purposes raises specific concerns in relation to children. Contrary to the storage of personal data in a row form (a face in photograph, a voice recording), such technologies rely on extracted personal characteristics that are saved as a template. A29WP emphasizes the need of appropriate safeguards in place against the risks of stigmatization or discrimination of children due to their age or their inability to enrol in biometric systems. It stated: "(t)he use of biometrics could impact significantly on the dignity, privacy and the right to data protection of vulnerable people

---

[813] Giovanni Sartor, Mario Viola de Azevedo Cunha; The Italian Google-Case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents. *Int J Law Info Tech* 2010; 18 (4): 356-378.

[814] Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 12 June 2009, WP 163, p. 8.

[815] The UK Information Commissioner (ICO) took a similar position regarding names and images: "*Religion or ethnicity, or both, can often be inferred with varying degrees of certainty from dress or name. For example, many surnames are associated with a particular ethnicity or religion, or both, and may indicate the ethnicity and religion of the individuals concerned. However, it would be absurd to treat all such names as "sensitive personal data", which would mean that to hold such names on customer databases you had to satisfy a condition for processing sensitive personal data. Nevertheless, if you processed such names specifically because they indicated ethnicity or religion, for example to send marketing materials for products and services targeted at individuals of that ethnicity or religion, then you would be processing sensitive personal data."* (UK Information Commissioner's Office. 'The Guide to Data Protection'. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf (30.03.2010), p. 24.

[816] FTC, 2011 Notice of Proposed Rulemaking (NPRM) to the Children's Online Privacy Protection Rule (COPPA), available at: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/16-c.f.r.part-312-childrens-online-privacy-protection-rule-proposed-rule-request-comment-proposal-amend-rule/110915coppa.pdf

[817] EPIC et al., Complaint to the FTC, 6 December, 2016, available at: https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf

[818] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies, 27 April 2012, WP 193.

such as young children […] to complete the enrolment process successfully. Given the potentially harmful consequences for the persons concerned, more stringent requirements will have to be met in the impact assessment process of any measure interfering with an individual's dignity in terms of questioning the necessity and proportionality as well as the possibilities of the individual to exercise his right to data protection in order for that measure to be deemed admissible."[819]

5.1.1.3. Geolocation data

Many geolocation data can be collected from children by their smart mobile devices through location sensors such as GPS or provided by children themselves, for instance, by geotagging of content on the Internet (e.g. embedding location in the videos and photos). For example, Flickr allows users to provide geolocation information or coordinates for their pictures with the help of a map interface. Geo-personalised services (including nearby places of interests), augmented reality, maps, geotagging, tracking the whereabouts of friends, looking for a person to date in the area, child control and location based advertising are just a few location based services used by children.[820]

The main risk to privacy related to the collection of location data stems from the fact that many other pieces of personal data can be derived from location data.[821] For example, it might be possible to infer the following: social relations between individuals, itinerary of a journey, points of interest related to hobbies, religious beliefs, political preferences or even potential diseases, movement patterns of an individual and mode of transport, the age or even the lifestyle, and mobility semantics.[822]

A recent revision of COPPA in the US explicitly included geolocation data among the protected categories of personal data of children. The FTC acknowledged that geolocation data (latitude and longitude coordinates, and may also include altitude, bearing, distance, and place names) is commonly embedded as hidden ''metadata'' within digital images and may be used by operators and accessed by the viewing public. COPPA covers the collection of geolocation information that is sufficient to identify the street name and the name of the town. It does not require the identification of the actual address using the information at the time of collection. When an application uses the child's longitude and latitude coordinates and locates them precisely on a map, COPPA protections would apply.

Empirical research indicates that many teenagers consider geolocation data sensitive. Pew Research Center found that around 46% of American teens have turned off location services on their cell phone or in an app because they were worried about other people or companies having access to that information.[823] Some of them were concerned about their own

[819] Ibid., p. 15.
[820] Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, 16 May 2011, WP 185.
[821] Jesús Friginal, Jérémie Guiochet, Marc-Olivier Killijian. AMORES L1.2 - A Privacy Risk Assessment Methodology for Location-Based Systems, Research Report, AMORES1.2/1.0; Rapport LAAS n° 16048, LAAS-CNRS, 2014, available at: hal-01282191
[822] Ibid.
[823] Pew Research Center, Teens and Mobile Apps Privacy, 2013, available at: http://www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_Teens%20and%20Mobile%20Apps%20Privacy.pdf

parents.[824] An earlier Pew Internet Project showed that about half of the parents of teens who owned cell phones monitored their child's location.[825]

5.1.1.4. Behaviour and habits

Behaviour and habits (repeated site visits, interactions, keywords, online content production, etc.) are the core elements observed by ad network providers in order to construct user profiles and serve them targeted advertisements. Advertisers can potentially gain a very detailed picture of a data subject's life online. Profiles can be the basis for taking decisions that significantly affect the child. Also, understanding of children can be manipulated by advertisers through various covert targeting techniques.[826] A recent EU study confirms this conclusion by showing that although the most popular online games (from 25 studied all advergames, all social media games and half of the games provided through popular application platforms) provide embedded or targeted contextual advertisements, children have difficulty in recognizing marketing intent of the content, in shielding themselves from it and in taking decisions.[827] The impact of embedded advertising is considerable on children from subliminally changing their behaviour and purchasing.[828] Also, increasingly sophisticated methods to gather children's data as they play, communicate or browse online, result in their constant surveillance. As Montgomery points out, the goal of these surveillance practices, that are used on many websites, is to create a cognitive, emotional and behavioural relationship between the child and the website, through micro-targeted 'one-on-one' marketing and communications strategies.[829] Similar worries about the commercial surveillance of children in networked spaces, and its subsequent effects, have been raised by a number of academics.[830]

Collection of geolocation information might also be used for user profiling through the collection of behavioural data. The provider of geolocation related services can gain an overview of habits and patterns of the child and create his extensive profile. Home, school and locations of other favoured places where a child travels regularly at certain times can be inferred.[831] Data derived from the movement patterns of friends (the so-called social graph) can also be linked to the profile of a child.[832] Given the vulnerability of children and the problems related to obtaining informed (parental) consent before a cookie or a similar device is placed or information stored in the user's terminal equipment, the Article 29 Working Party concludes that "ad network providers should not offer interest categories intended to serve

[824] Ibid.

[825] Amanda Lenhart, Rich Ling, Scott Campbell and Kristen Purcell, How parents and schools regulate teens' mobile phones, 20 April 2010, available at: http://www.pewinternet.org/2010/04/20/chapter-four-how-parents-and-schools-regulate-teens-mobile-phones/

[826] Fielder, A., Gardner, W., Nairn, A. and Pitt, J., Fair Game? Assessing commercial activity on children's favourite websites and online environments, UK National Consumer Council, 2008.

[827] European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behavior, March 2016, available at: http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/final_report_impact_marketing_children_final_version_approved_en.pdf

[828] Ibid.

[829] K. Montgomery, Youth and surveillance in the Facebook era: Policy interventions and social implications, *Telecommunications Policy* 2015 (39), 771-786.

[830] S. Grimes, Persistent and emerging questions about the use of end-user licence agreements in children's online games and virtual worlds. *UBC Law Review*, 2013 46 (3), 681-791; S. Grimes, Playing by the Market Rules: Promotional Priorities and Commercialization in Children's Virtual Worlds, *Journal of Consumer Culture 2015,* 15(1), 110-134; K. Montgomery, Youth and surveillance in the Facebook era: Policy interventions and social implications, *Telecommunications Policy* 2015 (39), 771-786.

[831] Article 29 Data Protection Working Party, Opinion 2/2010 on online behavioural advertising, 22 June 2010, WP 171.

[832] Ibid.

behavioural advertising or influence children"[833]. In the same vein, A29WP claimed that "behavioural advertising is "outside the scope of a child's understanding and therefore exceed the boundaries of lawful processing"[834].

The GDPR emphasises that specific protection should be provided to children against marketing or profiling (Recital 38). More specifically, children should not be subjected to automated decision making based on profiling (Recital 71). Similarly, COPPA in the US prohibits online tracking of children under the age of 13, including sharing of their data with third-party services such as ad networks and analytics services. Yet, in reality, research has demonstrated that "over 80% of the apps potentially used by children use at least one tracking service, as opposed to 65% of the apps falling in other app categories"[835]. The same research identified 19 games having more than 10 third-party tracking and advertising domains.[836]

Other specific data categories that might reveal behaviour and habits of a child and thus are to be considered in specific cases include, e.g., student data from educational institutions, including a child's attendance, progress in school, discipline, various assessment scores etc. and data related to juvenile offenders.

5.1.2. Attributes of Personal Data

Each data category relevant for the system under consideration should be described using the data attributes related to the nature of the data, the context, the purpose of data processing, control over data. These attributes are discussed below.

5.1.2.1. Sensitivity

The sensitivity attribute refers to whether the data is considered sensitive from the legal point of view. Children's personal data can be considered sensitive by its very nature. Although in Europe, neither the Directive 95/46/EC or the national data protection laws implementing it nor the General Data Protection Regulation (2016/679) explicitly include personal data of children among the sensitive data categories, there have been several suggestions to do so.[837] Nevertheless, specific safeguards and protections apply to children's data, showing its de facto sensitivity. The GDPR recognizes that children are vulnerable data subjects compared to adults, as "they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data", and thus deserve specific protection of their personal data (Recital 38). It constructs a specific, more restrictive protection regime for data controllers processing children's personal data: requires verifiable parental consent before processing personal data of children under the age of 16 (unless the Member States choose another age limit between 13 and 16) online, obliges data controllers to give information to children in a clear, audience-

[833] Ibid., p. 17.
[834] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices,* WP 202, 27 February 2013.
[835] Irwin Reyes et al., Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations, 2017, available at: http://eprints.networks.imdea.org/1557/1/conpro.pdf
[836] Ibid.
[837] European Commission before starting the revision of the Directive 95/46/EC considered extending the list of sensitive data categories to include minor's data, see European Commission, Stakeholders' Consultations "Future of data protection", Background paper, question 4, available at: http://ec.europa.eu/justice/news/events/data_protection_regulatory_framework/background_paper_en.pdf; Also, some Data Protection Authorities (DPAs) have proposed to add to the Directive 95/46/EC data of minors as an additional sensitive data category, Advice paper on special categories of data ("sensitive data"), available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf p.10.

appropriate language, restricts the use of the legitimate interest as a legal ground to justify data processing[838], and foresees additional safeguards in case of marketing and profiling. It clearly states that processing of children's personal data may lead to risks, of varying likelihood and severity, to children's rights and freedoms and cause harm (physical, material or non-material damage) (Recital 75).

5.1.2.2 Origin describing the data source

This data attribute relates to the origin of the data source, such as explicit disclosure by the subject, implicit disclosure (e.g. collection of IP address, MAC address, video-camera pictures), disclosure by a third party (e.g. friend), creation by the controller (e.g. inference). Explicit disclosure of personal data by an adult would be considered in compliance with the Directive 95/46/EC and the GDPR if, for example, based on transparent and clear information he or she provides free consent. In the case of children the validity of consent may be questioned.[839] The child-specific developmental needs and interests might have an impact on personal data sharing online. For example, as claimed by Steijn, behaviour of adolescents on social media (e.g. having more contacts, posting information more frequently) can be related to characteristics that are typical in their life stages (i.e. relationship development and identity development).[840] Peer pressure and the urge to explore one's identity also contributes to the tendency of sharing data and images on social networks.[841] In fact, oversharing of vast amounts of personal data online is common among children: on Facebook and Twitter 26% of youth publicly share their personal information, 14% even include address and telephone number in their profiles.[842] Children might not be aware of the long-term consequences of their sharing activities and realize the irretrievable and persistent nature of personal data posted online.[843] Moreover, not all children not able to understand and manage their privacy settings properly.[844] Default-settings (they rarely set the highest level of privacy protection), therefore, might have a direct influence on the online behavior and practices of children. Often children may not comprehend and skip reading privacy policies, especially because of their difficult language and length.[845] Services targeting or attracting children often fail to provide effective and reliable mechanisms through which parents can give their consent on behalf of their children.[846]

---

[838] Article 6 of the GDPR sates that data processing shall be lawful when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[839] S. Van der Hof, I Agree, or Do I: A Rights-Based Analysis of the Law on Children's Consent in the Digital World, 34 Wis. Int'l L.J., 2016, 409 - 445.

[840] W. Steijn, Developing a sense of privacy, Phd dissertation, Tilburg University, 2014, available at: https://pure.uvt.nl/ws/files/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf.

[841] Marwick, A., Murgia-Diaz, D. and Palfrey, J. (2010), "Youth, Privacy and Reputation" (Literature Review), *Berkman Center Research* Publication No. 2010-5, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1588163, p. 5.

[842] YPRT (Youth Protection Roundtable) (2009), *Stiftung Digitale Chancen*. Youth Protection Toolkit. Available at *www.yprt.eu/transfer/assets/final_YPRT_Toolkit.pdf*, 2009, p. 11.

[843] Ibid.

[844] Livingstone, Sonia and Ólafsson, Kjartan and Staksrud, Elisabeth, Social networking, age and privacy, EU Kids Online, London, UK, 2011.

[845] UK Children's Commissioner (2017) Growing up Digital: A Report of the Growing Up Digital Taskforce, January 2017.

[846] In 2015, 29 data protection authorities from around the world carried out a Global Privacy Sweep (i.e. a joint review of 1494 websites and apps directed towards children). In their final report they stated that "although many sites and apps claimed in their privacy policies to preclude access to children under a specified age, only 15% of websites and apps swept had age verification or gating to bar younger children from accessing

If children cannot fully control and comprehend explicit data disclosure online, implicit data disclosure (e.g. online tracking and profiling) is even more problematic. In fact, as noted above, data protection authorities consider that behavioural advertising, which is often based on the surreptitious use of cookies as web tracking devices, is "outside the scope of a child's understanding"[847].

In addition to excessive voluntary sharing, personal information can also be spread online by others. For example, 'tagging', i.e., a way to link a person to a picture, location or event, is an increased information sharing practice, often happening without consent from the persons concerned. Dooley et al. found that more than 40% of young people had pictures of themselves uploaded online without their permission[848], Lenhart observed that 6% of youth reported having an embarrassing photo of them uploaded online without their prior permission.[849] Sharenting is an emerging practice, when parents overshare the detailed information about their children on social networking sites without children's knowledge or consent.[850] Minkus et al. revealed that 35% of the 2,383 observed Facebook users publicly shared at least one photo of a child, while from the users in the age group of 30 to 49, 43% shared a photo of a child on their public pages.[851]

5.1.2.3. Purpose

Data processing systems can be created for different purposes. A distinction should be made between commercial and public or child best interest purposes of data processing (e.g. welfare, education, social security, health services). The purpose and the nature of the underlying relationship between the controller and the data subjects, whether it is commercial or otherwise, are important considerations in relation to legitimacy of the data processing.

The specific purpose of data processing is important when assessing possible negative impacts on data subjects and it is a prerequisite for other data quality requirements, such as adequacy, relevance and proportionality, accuracy and completeness, and requirements regarding the duration of data retention. Personal data can be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (Article 5 GDPR). In a narrow sense, in order for the purposes to be legitimate, the processing must at all times be based on at least one of the legal grounds provided for data processing, ranging from consent of the data subject to a balance of interests test (Article 6 Directive 95/46/EC and 6 GDPR). However, in a broad sense, the legitimate purpose also

---

the site or app. Sweepers also found that some of those controls did not function (e.g., a child indicating she was 10 years old could still access the site) and others were only passive (e.g., a pop-up indicating that a child below a specified age should not access the site). Noteworthy, only 24% of sites and apps swept encouraged parental involvement." GPEN, '2015 GPEN Sweep - Children's Privacy', 2015, available at: http://194.242.234.211/documents/10160/0/GPEN+Privacy+Sweep+2015.pdf

[847] Article 29 Data Protection Working Party, *Opinion 02/2013 on apps on smart devices,* WP 202, 27 February 2013.

[848] Dooley, J.J., Cross, D., Hearn, L. and Treyvaud, R., "Review of existing Australian and international cyber-safety research". Child Health Promotion Research Centre, Edith Cowan University, Perth, 2009, available at www.dbcde.gov.au/__data/assets/pdf_file/0004/119416/ECU_Review_of_existing_Australian_and_international_cyber-safety_research.pdf, p. 11

[849] Lenhart, Amanda, Cyberbullying and Online Teens, Pew Internet & American Life Project, 27 June 2007, available at: http://www.pewinternet.org/PPF/r/216/report_display.asp

[850] Stacey Steinberg, "Sharenting: Children's Privacy in the Age of Social Media" University of Florida Levin College of Law Legal Studies Research Paper Series Paper No 16-41, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711442

[851] Tehila Minkus, Kelvin Liu and Keith W. Ross, Children Seen But Not Heard: When Parents Compromise Children's Online Privacy, 2015, available at: http://cse.poly.edu/~tehila/pubs/WWW2015children.pdf

"requires that the purposes must be in accordance with all provisions of applicable data protection law, as well as other applicable laws such as employment law, contract law, consumer protection law"[852]. This means that when determining whether a particular purpose is legitimate data controllers should consider all forms of written and common law, constitutional principles, fundamental rights, jurisprudence, and other elements such as codes of conduct, codes of ethics, and the general context and facts of the case.[853] The list of child rights provided earlier in this paper thus constitutes one of such considerations. Consumer protection law, in particular the rules on unfair commercial practices and vulnerable consumers, is another important source of law to be considered. For example, the use of certain techniques such advergames can have a manipulative effect with such techniques often implementing personal data gathering as part of the commercial offering.[854] Given the gamification of the personal data collection it is arguable that such a technique could fall foul of the fairness test in the Unfair Commercial Practices Directive.[855] Also more generally, due to the vulnerability of children, the collection of their personal data for direct advertising purposes may result in the personalisation having an undue influence on the decision-making capacity of the child. Therefore, the collection of data of children who have not reached a sufficient degree of maturity for marketing purposes has been declared as illegitimate by some data protection authorities.[856] Similarly, the Article 29 Working Party has made it clear that direct marketing should not be aimed at children and that data (e.g. data about children's interests) should not be collected from children with the purpose to serve behavioural advertising or influence them.[857]

Data controllers should not only ensure that the purpose for data processing is legitimate, but also that any further processing is compatible with the initially specified purpose. Purpose compatibility should be more rigidly evaluated when data controllers process personal data of children.[858]

5.1.2.4. Retention

This data attribute relates to the period of time after which the data will be deleted. Irrelevant data cannot be retained by the data controllers (Article 6(e) Directive 95/46/EC and 5(1e) GDPR). As noted by the A29WP, "(b)ecause children are developing, the data relating to them change, and can quickly become outdated and irrelevant to the original purpose of collection".[859]

Data retention is affected by an enhanced possibilities that the GDPR provides for children to erase their personal data (Article 17 GDPR). The right to erasure ("right to be forgotten") is

[852] Article 29 Working Party, Opinion 03/2013 on purpose limitation, 2 April 2013, WP 203, p. 20.
[853] Ibid.
[854] V. Verdoodt, D. Clifford, E. Lievens, Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU, 32 Computer Law & Security Review, 2016, 599 – 614.
[855] Directive 2005/29/EC of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive), 11.06.2005, L149/22.
[856] Opinion 38/2002 of the Belgian Data Protection Authority relating to the protection of the privacy of minors on the Internet, availabe at: http://www.privacycommission.be/sites/privacycommission/files/documents/avis_38_2002.pdf, p. 5.
[857] See Article 29 Data Protection Working Party Opinion 5/2009 on online social networking, 12 June 2009, p. 12, Opinion 2/2010 on online behavioural advertising, 22 June 2010, p. 17.
[858] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160, 11 February 2009.
[859] Ibid.

particularly aimed at children in online environments, when their data is collected based on consent, and allows children to remove personal information that may be damaging to their reputation and personality. It can be exercised even if an individual is no longer a child.

5.1.2.5. Intervenability

Intervenability refers to control over data and the possibilities for the data subject to exercise his rights (access, modification, deletion, challenge, etc.). The rights of children as data subjects (the right to be informed, the right of access and correction/deletion/blocking, and the right to object) are the same in their nature as the rights of adults, but are particular in terms of their (often indirect) exercise. Access to the child's personal data and consequently other rights will normally be exercised by the child's representative, i.e. his parent or legal guardian, but as noted by the Article 29 Working Party, in some circumstances the child's right to privacy may prevail over the representative's right of access.[860] Data controllers should always take into consideration the best interests of the child, national laws, the age of the child and who - the child or the representative - provided the data. The latter indicates the degree of child's maturity and autonomy. In the UK, for example, children from the age of 12 can exercise their right of access alone[861], but in many other EU Member States this age limit is not explicitly defined. Therefore, not providing a child (when he is mature enough) the possibility to update, modify, correct or challenge incorrect or outdated data about himself might create a stronger possibility of a feared event of inaccurate data processing.

In contrast to adults, children may not be aware of their data subject's rights. Therefore, data controllers are required to inform the child of their rights in a clear and accessible language.

When the data subject has the right to object to the processing on compelling legitimate grounds (when data is processed based on Art 7 e) and f) of Directive 95/46/EC) these grounds can be particularly compelling in case of children.[862]

5.2. Risk Sources

A risk source is any entity (individual or organization) which may process (legally or illegally) data belonging to a data subject and whose actions may directly or indirectly, intentionally or unintentionally lead to privacy harms. The literature often refers to the adversary or the attacker. But, here, we prefer to use the term "risk sources" as it is less security connotated and is not limited to malicious actors. In the following, we first discuss the categories of risk sources that are especially relevant for children (Section 5.2.1) before presenting the relevant attributes (Section 5.2.2).

---

[860] Ibid.

[861] UK Data Protection Act 1998 has a special section on the exercise of rights in Scotland by children which states: "where a question falls to be determined in Scotland as to the legal capacity of a person under the age of sixteen years to exercise any right conferred by any provision of this Act, that person shall be taken to have that capacity where he has a general understanding of what it means to exercise that right." It further specifies: "a person of twelve years of age or more shall be presumed to be of sufficient age and maturity to have such understanding".

[862] See the data subject's right to object in Article 14 of the Directive 95/46/EC and Article 21 of the GDPR

5.2.1. Categories of risk sources

The general categories of risk sources to be considered are: insiders (eg., system administrator, employee), outsiders (eg., users of the system), the data controller itself, governments and law enforcement bodies, criminals and other organizations. These categories can be derived from actors and interface attributes of the system, the data flow view attribute of the stakeholders and the categories of data involved. The actors attribute specifies various roles in the organization of the data controller that may act as risk sources. The interface attribute determines the contact points between the system and the external world and hence helps identifying the potential risk sources outside the system, such as hackers, friends, acquaintances or family of data subjects, etc. The data flow view identifies different stakeholders that handle the data and enables to identify stakeholders such as third parties, other data subjects, data processors and data controllers themselves as potential risk sources.

The specific categories of risk sources that are relevant to children's data processing systems are data controllers themselves and related third parties, outsiders like hackers, trusted individuals like friends, family members or others with whom the child may interact frequently, such as teachers. For example, third parties like ad network providers can be classified as risk sources as they collect, aggregate and link children's personal data in order to create their profiles.

Two particular risk sources merit further discussion in the case of children. First, friends are normally very closely trusted by children and thus they might often have a detailed background information about the data subject. Steeves et al.[863] show that youth do not think it is risky to share email addresses and passwords with their friends. Disclosure of personal data easily becomes a mean to maintain intimate relations with friends.[864] A way for friends to control the social networking sites on behalf of password owners is a demonstration of trust similar to telling to a friend a combination for a locker in the offline world.[865]

Yet, the notion of friends itself should be critically assessed in the digital context. As Livingstone asserts, youth "work with a subtle classification of 'friends', graded in terms of intimacy, which is poorly matched by the notion of 'public' and 'private' designed into social networking sites."[866] Ties between friends on social networks can be weak.[867] Children, especially teenagers, view different social environments as multiple and possibly overlapping, making distinction between various groups of friends, parents, future employers, a process called "audience segregation".[868] They create and use different partial identities according to different contexts.[869]

Second, in specific circumstances children have the right to privacy against their own parents. The complexity of privacy boundaries within the family have been evidenced by academics.[870] As a result, parents although being the primary representatives of children and

[863] V. Steeves and C. Webster, Closing the barn door: the effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology & Society*, 2008, 28(1), p. 419.
[864] Ibid.
[865] Ibid.
[866] S. Livingstone, Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. New Media Society, 2008, 10(3), 393-411, p. 404.
[867] Gross, Ralph, and Alessandro Acquisti, Information revelation and privacy in online social networks, *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM, 2005.
[868] B. van den Berg, R. Leenes, Keeping Up Appearances: Audience Segregation in Social Network Sites. In: Gutwirth S., Poullet Y., De Hert P., Leenes R. (eds) Computers, Privacy and Data Protection: an Element of Choice. Springer, Dordrecht, 2011.
[869] danah boyd, *It's Complicated: the Social Lives of Networked Teens*, New Haven, CT: Yale University Press, 2014.
[870] Newell BC, Metoyer C and Moore AD (2015) Privacy in the family. In: Roessler B and Mokrosinska D (eds) *Social Dimensions of Privacy: Interdisciplinary Perspectives*. Cambridge: Cambridge University Press, pp.

their interests, can also potentially invade their own children's privacy and become risk sources. For example, by using the right of access to personal data on behalf of their (more mature) children, parents could learn about their children's online activities. Also, parents can sell or publish children's personal data breaching the privacy of their children. In this case, children might have difficulties in exercising their right to delete their data and lodge a complaint as they need a legal guardian. To protect their right to privacy, children who are mature enough to understand that their privacy has been breached, should have the right to be heard by data controllers and competent authorities.[871]

5.2.2. Attributes of risk sources

Each risk source must be described using the following attributes. The first attribute is the relationships between the risk sources and different stakeholders. Such relationship can be defined as 1) insider / outsider, describing whether the risk source works within the data controller organization or not; 2) individual / organization describing whether the risk source acts as an individual or as an organization; 3) the relationship with data subjects describing trust relationships between risk sources and data subjects. For example, a friend or a family member is usually trusted by the data subject, whereas limited trust is placed on the service provider or a service technician.

The second attribute is the level of motivation of the risk source. Such motivation can relate to the potential value of the privacy breach for the risk source (e.g., financial benefit, retaliation, thrill, etc.) and all incentives and dis-incentives (e.g., the risk of being caught).

The third attribute refers to resources available to the risk source. Background information, i. e., additional information available to the risk source, may help it to carry out a privacy breach (e.g., detailed knowledge of the system, security flaws, etc.). Other attributes that should be considered are access rights to different types of data being processed by the system (for e.g., a system administrator may already have access to some data whereas other employees do not) and tools or skills, and computation power available to the risk source.

The values of some of the above attributes such as insider/outsider, individual/organization and relationship with data subjects can influence the values of other attributes such as background information, motivation/fear, access rights, etc. The fact that the risk source is an insider or outsider can strongly determine whether it possesses access rights to personal data, background information and also influences the nature of tools/skills or computation power it possesses and its possible motivation/fear.

A system administrator in charge of a critical sub-system can be assumed to have extensive knowledge about the system including its weaknesses and may have been given access rights to personal data processed by the system. However, being in such a responsible position, he may be subject to constant scrutiny (possibly at a higher level than other employees) and hence, expect high chances of getting caught and fear losing his job and other severe punishments if he tries to exploit a privacy weakness. Similarly, a risk source's relationship with the data subject strongly determines the background information he has and also influences his motivation/ fear. For example, as discussed above, friends may be deemed more trustworthy by a chid (making him prone to share secret information such as passwords than by an adult. Also, when a data subject is a child a close family member may be able to have substantially more background information about a child than in the case of an adult data subject. Family members may even have information about the child about which the child

104–121. Shmueli B and Blecher-Prigat A (2011) Privacy for children. *Columbia Human Rights Law Review* 42: 759–795.

[871] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160, 11 February 2009.

himself is not well aware (e.g., health data). However, family members will generally have less motivation to invade children's privacy. If the risk source is an organization (such as a third party), it may have high financial motivations to, for example, re-identify anonymized data to utilize it for its own business purposes. Risk sources backed by an organization will also generally have higher financial and technical resources and hence possess better tools/skills and computation power than individual risk sources.

The value of a privacy breach for a risk source is influenced by the data attributes precision, sensitivity and volume. Sensitive data such as financial data, health data definitely have more appeal to a risk source. Similarly, high volume and precision data may be attractive to a risk source because of the possibilities of data inference that they provide.

5.3. Feared events

A feared event is an event of the system that might occur as a result of the exploitation of one or more privacy weaknesses and may lead to privacy harms. We introduce a distinction between feared events which are "technical events" and privacy harms (defined in the next section) which correspond to the impact of feared events on people. In the following, we first discuss the exemplar categories of feared events that are especially relevant for children (Section 5.3.1) before presenting the relevant attributes (Section 5.3.2).

5.3.1. Categories of feared events

Categories of feared events that a privacy analyst should consider when processing personal data are closely related to the data protection principles and the grounds for lawful data processing listed in the data protection law.[872] The most relevant examples of the categories of feared events in applications and services requested and delivered over the internet (information society services) that process children's data include:

1) Excessive data collection (e.g., collection of data from children regarding members of their family, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refers). Excessive data collection could infringe the principles of purpose limitation and data minimisation[873]. These principles require to process personal data only for specified, explicit and legitimate purposes and collect adequate, relevant and limited to the specified purposes data.
2) Unauthorized access to data (e.g., access to data by hackers) and unauthorised modification of data (e.g., modification of data by the service provider). Lack of appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, would infringe the principle of data integrity and confidentiality[874].
3) Use of data for unauthorized purposes (e.g., use of browsing data by the data controller to build detailed profiles) and unjustified data inference or re-identification (e.g., inference about child's sleeping patterns from Facebook access data). Processing of personal data for unspecified or incompatible purposes with the initially defined purposes could infringe the principle of lawfulness, fairness and transparency and the

[872] Articles 6 and 7 of the Directive 95/46/EC, Articles 5 and 6 of the GDPR.
[873] Article 5 Part 1 (b) and (c) of the GDPR.
[874] Article 5 part 1 (f) of the GDPR

principle of purpose limitation.[875] Fairness and transparency require specific and more rigid interpretation in the case of children's data processing, as discussed below.

4) Storage or use of inaccurate data (e.g., not providing children the ability to update, modify, correct or challenge incorrect or outdated data about himself). Processing of outdated or otherwise inaccurate personal data could infringe the data accuracy principle.[876] Accuracy of children's personal data can change particularly quickly due to their growth. If no easy way to access and correct or delete inaccurate personal data is ensured by the data controller, data subject's rights might be also violated.[877]
5) Disclosure of data to unauthorized actors or unauthorized publication (e.g., data controllers giving access to data to third parties without data subject's consent or with expired parental consent as the child reached the age at which he can consent). Unauthorised data disclosure to third parties would infringe the principle of lawful, fair and transparent data processing.[878]
6) Retaining data more than necessary (e.g. lack of deletion or ineffective deletion of personal data). Unnecessary data storage could contradict the storage limitation principle, which requires to store personal data no longer than necessary for the purposes for which the data were collected.[879] It is allowed to process personal data, however, for longer periods in specific cases, e.g. archiving purposes in the public interest, scientific, historical research or statistical purposes, under defined conditions.

In relation to children's personal data, particular attention should be paid to the interpretation of some principles relating to the processing of personal data and the grounds for lawful data processing. First, the principle of fairness must be awarded a broader scope when children's data is processed.[880] It requires not only to collect data in a transparent manner but also to act with the utmost good faith, such as to handle personal data only in ways data subjects would reasonably expect and not to use personal data in ways that unjustifiably causes a negative impact on individuals.[881] For example, on an individual level, a "derogatory, threatening and abusive online postings" by organisations or individuals acting for non-domestic purposes, can be considered unfair[882]. In a commercial context, deceptive or manipulative data collection practices from children (e.g. advergames, manipulative and aggressive tracking) would be unfair.

Second, to comply with the lawfulness requirement data controllers need to rely on an appropriate legal ground for children's data processing. The most common legal ground is data

[875] Article 5 part 1 (a) and (b) of the GDPR.
[876] Article 5 part 1 (d) of the GDPR
[877] Articles 12-22 of the GDPR
[878] Article 5 part 1 (a) of the GDPR.
[879] Article 5 part 1 (b) of the GDPR.
[880] Bygrave defines fairness as a principle: "at a very general level, the notion of fairness undoubtedly means that, in striving to achieve their data processing goals, data controllers must take account of the interests and reasonable expectations of data subjects; controllers cannot ride roughshod over these. This means that the collection and further processing of personal data must be carried out in a manner that does not, in the circumstances, intrude unreasonably upon the data subjects' privacy nor interfere unreasonably with their autonomy and integrity. In other words, fairness requires balance and proportion. These requirements are applicable not just at the level of individual data processing operations; they are equally applicable to the way in which the *information systems* supporting such operations are designed and structured." Lee A Bygrave, Core principles of data protection, 7(9) Privacy Law and Policy Reporter, 2001, 169.
[881] UK Information Commissioner's Office, The Guide to Data Protection, 11 May 2016, available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-4.pdf On the detailed discussion of the principles of fairness in data protection law also see D. Clifford and J. Ausloos, 'Data Protection and the Role of Fairness', CiTiP Working Paper 29/2017, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3013139
[882] ICO, Social networking and online forums–when does the DPA apply?, Data Protection Act

subject's consent. For this ground to be valid consent has to be freely given, specific, informed and unambiguous. Where services requested and delivered over the internet are directed to a child under 16 years old (unless a Member State's national laws set a lower age which cannot go below the age of 13), processing of his personal data is lawful only if consent is given or authorised by the holder of parental responsibility over the child (Article 8 GDPR). To acquire a valid parental consent, the data controller has to reliably establish that a child is under the default age of consent (i.e. to verify child's age) and to make reasonable efforts to ensure that consent was given by a parent or a legal representative.

Third, data controllers should make extra efforts to guarantee transparency for children. Children, and even many adults, encounter difficulties in reading and understanding privacy policies. Bonneau and Priebusch in their assessment of privacy policies of social networking sites showed "great diversity in the length and content of formal privacy policies" and, evidenced that "almost all policies are not accessible to ordinary users due to obfuscating legal jargon".[883] As one could expect, users are reluctant to read such complex and long documents. A recent Eurobarometer survey in EU Member States showed that 56% of internet and online-platform adult users do not read terms and conditions at all while a further 18% read them without taking them into account.[884] As a result, "if a child lacks the knowledge or understanding of data protection rules then they are unlikely to appreciate that SNSs are processing their personal data when they post it online, nor are they likely to appreciate that some personal data is considered "sensitive" and should be subject to more stringent processing conditions (for example, if they upload a photo of a Hanukkah celebration)".[885]

The GDPR obliges data controllers to give information to all data subjects in clear, audience-appropriate language before their personal data is collected. Recital 58 of the GDPR frames this requirement in relation to children as giving information 'in such a clear and plain language that the child can easily understand'. This means that a full privacy policy providing detailed information to users about the processing of their personal data should be always available but that in addition service providers should create notices that are meaningful and meet the specific needs of children in the target group of the service. In other words, child-adapted information should be complementary and cannot be used as a substitute when implementing the requirement[886] - for which data controllers are held accountable - to provide detailed information to data subjects according to EU data protection law.[887] As regards the form of child-appropriate information, data controllers should adapt information to the child's level of maturity.[888]

A broad range of suggestions has been made on how to improve the understanding and readability of the information provided to the users in general, such as "multi-layered" privacy

[883] Joseph Bonneau and Sören Preibusch, The Privacy Jungle: On the Market for Data Protection in Social Networks, the Eighth Workshop on the Economics of Information Security, London, 24 June 2009, available at: http://www.jbonneau.com/doc/BP09-WEIS-privacy_jungle.pdf

[884] European Commission, "Special Eurobarometer 447: Online platforms" (June 2016), availabe at: http://ec.europa.eu/information_society/newsroom/image/document/2016-24/ebs_447_en_16136.pdf, 65

[885] Karen Mc Cullagh, The General Data Protection Regulation: a partial success for children on social network sites?', in Tobias Bräutigam and Samuli Miettinen (eds.) *Data Protection, Privacy And European Regulation in the Digital Age*, Unigrafia, Helsinki, 2016.

[886] Article 10 of Directive 95/46/EC and Article 13 of the GDPR require to provide detailed information to users about the processing of their data, describing, amongst others, the processing activities that data controllers may carry out (such as further using the data for profiling, data mining, etc), the rights of individuals and how they can exercise them.

[887] EDPS, Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", 17 July 2012.

[888] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160, 11 February 2009.

notices[889] or visceral notices[890]. Less has been written on how to adapt the information to children's needs.[891] One of the suggestions, made by the European Commission, to the industry is to implement "contextual information" of every piece of personal data collected to set up an online profile.[892] The European Data Protection Supervisor (EDPS) has clarified that such "contextual information" could mean that service providers inform children about "the level of sensitivity of each piece of information they provide when creating an online profile" and about "potential risks or harms they may encounter with the disclosure of such information to a restrained, larger or indefinite number of people".[893] For this purposes, the EDPS has suggested, that industry could develop a common taxonomy to explain the level of such potential harms (e.g. the possible harm that might be caused by the acceptance of cookies, profiling or identification) and sensitivity of each piece of personal data.[894] Another possibility for creating child-adapted privacy policies and testing their comprehensiveness among children is to involve children themselves. Academics have shown that children's participation is particularly useful in identifying transparency and privacy issues in order to consider their implications in the reformulation of privacy policies.[895] Innovative mechanisms, such as participatory design, co-creation sessions or collaborative platforms can be used for developing child adapted information and protection tools.[896]

Consultation with children as key stakeholders and the incorporation of their views, needs and interests in all the matters affecting them is a requirement under Article 12 of the UN CRC. It is also a recommendation for industry issued by the ITU[897] and part of the Corporate Social Responsibility in relation to respect for human rights. [898]

5.3.2. Attributes of feared events

The first important attribute of a feared event is its scale. Scale refers to the number of potential individuals whose personal data is concerned by a feared event. For example, public

[889] Article 29 Working Party, Opinion 10/2004 on more harmonised information provisions, WP 100. Noain-Sánchez, (2015).
[890] Calo (2012), 1033.
[891] EDPS (2012), Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", 17 July 2012.
[892] European Commission, Communication on a "European Strategy for a Better Internet for Children", COM (2012) 196 final.
[893] Ibid, p.8.
[894] Ibid., p. 7.
[895] A. Micheti, J. Burkell, V. Steeves, Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand, Bulletin of Science, 30 Technology & Society, 2010; V. Donoso, M. van Mechelen, V. Verdoodt, Increasing User Empowerment through Participatory and Co-design Methodologies, Emsoc project deliverable D1.3.1c, 2014, available at: http://emsoc.be/wp-content/uploads/2014/09/D1.3.1c_ICRI1.pdf; S. Coleman, K. Pothong, E. Perez Vallejos, A. Koene, Internet On Our Own Terms: How Children and Young People Deliberated About Their Digital Rights, 2017, available at: http://casma.wp.horizon.ac.uk/casma-projects/5rights-youth-juries/the-internet-on-our-own-terms/
[896] E. Lievens, Children's rights and media: imperfect but inspirational, E. Brems, W. Vandenhole and E. Desmet (eds.), Children's Rights Law in the Global Human Rights Landscape**:** Isolation, inspiration, integration?, Routledge, 2017.
[897] ITU, Guidelines for industry on child online protection, 2014, available at: www.itu.int/en/cop/Documents/bD_Broch_INDUSTRY0809.pdf
[898] UN Guiding principles on business and human rights, The children's rights and business principles, UN Global Compact, UNICEF and Save the Children 2013. The Committee on the Rights of the Child, General Comment on State obligations regarding the impact of the business sector on children's rights. Council of Europe, 'Recommendation of the Committee of Ministers to member states on human rights and business', 2016.

data disclosure may happen for some, but not all users, since not all users use the default privacy setting. However, if the data controller discloses data intentionally to third parties it may do so for all users. This attribute should not be confused with the victims attribute of the harm component. Usually, the number of victims of a feared event is smaller than the number of victims of the corresponding harm. For example, behavioral trends observed for a small group of individuals (victims of the feared event) of a particular age or gender may often be generalized for all individuals (victims of the harm) belonging to the same group.

A second attribute of a feared event is irreversibility, i.e., the difficulty with which the feared event can be reversed. Two main factors influence irreversibility: the extent of exposure of the personal data and the technical difficulty to reverse the effect of a feared event. As to the first factor, it may be difficult to remove all traces of personal data once disclosed to the public online. The second factor depends on the intervenability attribute of the data. The settings of a social networking site may be poorly designed thus becoming a technical obstacle for a child who wants to remove an embarrassing information about him posted by a friend.

5.4. Privacy Weaknesses

A privacy weakness is a weakness in the data protection mechanisms (whether technical, organizational or legal) of a system or lack thereof that can ultimately result in privacy harms. Privacy weaknesses include: 1) weaknesses introduced by design choices or choices of functionalities; 2) system design errors and 3) implementation errors. Privacy weaknesses due to implementation errors or design flaws are akin to vulnerabilities in traditional computer security. Privacy weaknesses due to design choices or the definition of the functionalities of the system itself are specific to privacy. Typically, the excessive collection of data can be a deliberate choice (either at specification time or at design time) to accumulate data that could be exploited in the future. In the following, we discuss the categories of privacy weaknesses (5.4.1) that are especially relevant for children and their attributes (5.4.2.).

5.4.1. Categories of privacy weaknesses

Specific categories of potential privacy weaknesses of the systems processing children's data are the following:

- Inappropriate interface that is difficult to understand or misleading for a child

Specific design choices that are not user-friendly and implemented into the system can facilitate excessive personal data disclosure. For example, empirical research shows that children experience problems in finding privacy protecting tools, such as privacy settings to limit personal data sharing. According to the Net Children Go Mobile project, only around half (55%) of 11-13 years old children in Europe are able to change the privacy settings of their social network profiles.[899]

As a result, privacy by design and the use of Privacy Enhancing Technologies are particularly important in data processing activities targeting children. One of the essential requirements is the implementation of age-appropriate privacy settings by default. Although basic default settings should be embedded by default for all users, such settings for children

[899] Giovanna Mascheroni and Kjartan Ólafsson, *Net children go mobile: risks and opportunities* (2nd edn Educatt, Milan 2014)

should be more protective.[900] The EDPS has noted, for example, that "it would be particularly appropriate to have specific settings implemented on online social networking sites used by children, such as a tool checking the age of friends before a child can accept them, combined with settings providing for an additional check by the parents or the legal guardians of children, to validate in order to get adult friends."[901] When designing the system, attention should be paid not only to the initial default settings, but also to their changes which should be accompanied by clear information and warnings in a clearly understandable language for children about the impact and potential harms.[902] Also, the possibility to change the default settings should be related to the age and maturity of the child and when necessary parental consent should be obtained before a child can change the default settings.[903]

- Excessive data collection through age and parental consent verification mechanisms

Some age and consent verification implementations may lead to excessive data collection of a large number of both children and adults, and diminish anonymity online. For example, instead of verifying that an individual is above a certain age threshold the data controller asks for the exact age of a person or even fully identifies an individual based on his age and other pieces of personal data (name, ID number, etc.).

- Unauthorised data collection by third parties

For instance, the surreptitious use of cookies as web tracking devices would undoubtedly be an unauthorised collection of personal data given that consent as defined in the GDPR is required as per Article 5(3) e-Privacy Directive.[904] Moreover, given that the e-Privacy Directive relies on the definition of consent as provided for in the GDPR, it is also unclear how a child could consent to the placing of information or the accessing of information already stored (such as a cookie) on the terminal equipment of the user. As such, in the context of services directed towards children one must question whether such technologies are in fact permissible outside of the two exemptions provided for in the e-Privacy Directive (i.e. for functional cookies) given the requirements relating to parental consent. In addition, one must also wonder how the cookie consent rules will apply in practice to general services which although not specifically targeted to children are often used by them.

5.4.2. Attributes of privacy weaknesses

5.4.2.1. Exploitability

Exploitability values of some relevant privacy weaknesses of the system can be:

1. Low means difficult to exploit (for e.g., the associated data is encrypted, not visible to many actors or properly de-identified, the concerned supporting assets are difficult to access by risk sources);

[900] EDPS (2012), Opinion on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - "European Strategy for a Better Internet for Children", 17 July 2012.
[901] Ibid.
[902] Ibid.
[903] Ibid.
[904] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive), Official Journal [2002] OJ L 201/37.

2. Medium means exploitable with moderate difficulty (e.g., the associated data is unencrypted but is of low volume and precision or not properly de-identified, the concerned supporting assets are moderately difficult to access by risk sources);

3. High means easily exploitable (e.g., the associated data is unencrypted, is of high volume or precision, not de-identified at all, the concerned supporting assets can be very easily accessed by risk sources, associated data is visible to risk sources, no possibilities of intervention by data subject, etc.).

The values are assumed to be assigned by a privacy expert.

5.5. Privacy Harms

Privacy harm assessment is the ultimate goal of the analysis. A privacy harm is the negative impact on a data subject, or a group of data subjects, or the society as a whole, from the standpoint of physical, mental, or financial well-being or reputation, dignity, freedom, acceptance in society, self-actualization, domestic life, freedom of expression, or any fundamental right, resulting from one or more feared events. In the following, we first discuss the categories of privacy harms that are especially relevant for children (Section 3.5.1) before presenting the relevant attributes (Section 3.5.2.).

5.5.1. Categories of privacy harms

The relevant privacy harms are derived from the feared events and external factors such as societal norms, legal environment, etc. The following categories of harms have been identified in previous works[905] and should be considered in the DPIA:

5.5.1.1. Physical harms

Physical harms are linked to physical ailments, death, injury, etc. For example, a criminal may stalk and injure a child or a sexual predator may exploit a child after coming to know his precise location every evening from check-ins posted by the individual on a social networking site. In one of the few cases directly related to personal data of children online brought before the European Court on Human Rights (ECtHR) K.U. v. Finland, when physical and moral welfare of a child was threatened the ECtHR emphasised the vulnerability of children.[906] KU, a 12-year old applicant, lodged a complaint because an unknown person placed an advertisement on a dating site on the internet in his name, without his knowledge. The advertisement included KU's personal data, such as age and year of birth, gave a detailed description of his physical characteristics and provided a link to his web page with his picture. In the advertisement, it was claimed that KU was looking for an intimate relationship with a boy of his age or older. The ECtHR emphasized 'the potential threat to the applicant's physical

[905] Ryan Calo. Boundaries of Privacy Harm, The. Ind. LJ, 86:1131, 2011; Julie E Cohen. Examined lives: Informational privacy and the subject as object. Stanford Law Review, pp. 1373–1438, 2000. Paul M Schwartz. Privacy and democracy in cyberspace. Vand. L. Rev., 52:1607,1999. Paul M Schwartz and Daniel J Solove. PII Problem: Privacy and a New Concept of Personally Identifiable Information, The. NYUL Rev., 86:1814, 2011. Daniel J Solove. A taxonomy of privacy. University of Pennsylvania law review, pages 477–564, 2006.

[906] App no. 2872/02, 2009, 48 EHRR 52.

and mental welfare (…) and his vulnerability in view of his young age' (he was aged 12 at the time of the alleged infringement). Due to the advertisement, the child became a potential target of paedophiles, and therefore, there was a risk of physical and mental harms occurring.

5.5.1.2. Economic or financial harms

Economic harms can be loss or damage of property, unanticipated financial loss, etc. For example, from vacation pictures posted on a social networking sites burglars may infer when the home is empty. Behavioral profiling might also be seen as causing economic harms to consumers as advertisers might offer goods at different prices and set a maximum price on an individual base for each consumer.[907]

5.5.1.3. Mental or psychological harms

Mental and psychological harms constitute fear of misuse of personal data, fear of being observed, fear of being treated unfairly, anxiety, mental distress, etc. Occurrence and negative effects of these type of harms online is high among children, especially in the context of cyberbullying and cybervictimisation.[908] Research estimates that from 20 to 40 percent of children and adolescents have experienced cyberbullying.[909] There is an extensive body of research on cyberbullying, showing very serious effects on the adolescents who become victims of cyberbullying. Cyberbullying has been linked with the following harms: an increase in anxiety[910], low self-esteem[911], depression[912], suicidal ideas[913]. Some national studies, in addition, found associations between cyberbullying and the psychological and emotional effects of 'confusion, guilt, shame, self-harm, distress and withdrawal from friends'.[914] As a result of the negative effects, negative consequences can also be noted in learning due to the association of cyberbullying with concentration problems, poor performance at school.[915]

Academics define cyberbullying underlining some of its specific elements, such as the use of electronic means, intentional harm, imbalance of power, repetition, sense of anonymity

[907] FTC, How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population, 2014, available at: https://www.ftc.gov/system/files/documents/public_comments/2014/08/00015-92370.pdf

[908] David Álvarez-García, José Carlos Núñez, Alejandra Barreiro-Collazo, Trinidad García, Validation of the Cybervictimization Questionnaire (CYVIC) for adolescents, Computers in Human Behavior, 2017 (70), 270-281.

[909] E. Aboujaoude, M.W. Savage, V. Starcevic, W.O. Salame, Cyberbullying: Review of an old problem gone viral, Journal of Adolescent Health, 2015, 57 (1), pp. 10-18.

[910] Ch A. Rose, B.M. Tynes, Longitudinal associations between cybervictimization and mental health among U.S. adolescents, Journal of Adolescent Health, 20015, 57 (3), pp. 305-312

[911] F.C. Chang, C.M. Lee, C.H. Chiu, W.Y. Hsi, T.F. Huang, Y.C. Pan, Relationships among cyberbullying, school bullying, and mental health in Taiwanese adolescents, Journal of School Health, 2012, 83 (6), pp. 454-462

[912] R.A. Bonanno, S. Hymel, Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying, Journal of Youth and Adolescence, 2013, 42, pp. 685-697.

[913] M. Van Geel, P. Vedder, J. Tanilon Relationship between peer victimization, cyberbullying, and suicide in children and adolescents. A meta-analysis, JAMA Pediatrics, 2014, 168 (5), pp. 435-442.

[914] Baker, Ö., & Tanrikulu, I. Psychological consequences of cyber bullying experiences among Turkish secondary school children. Procedia – Social and Behavioral Sciences, 2010, 2(2), pp. 2771–2776.

[915] A. Tsitsika, M. Janikian, S. Wójcik, K. Makaruk, E. Tzavela, C. Tzavara, *et al.* Cyberbullying victimization prevalence and associations with internalizing and externalizing problems among adolescents in six European countries, Computers in Human Behavior, 51 (2015), pp. 1-7.

and lack of accountability.[916] Cyberbullying may have many different forms and only some of its forms coincide with data protection violations. These forms are fraping and impersonating (logging into the victims social networking account and impersonating him by posting inappropriate content), catfishing (stealing online identities, e.g. photos, and creating social networking profiles for deceptive purposes).[917] Another phenomenon of this type, ironically called as "happy slapping", refers to the recording of a physical attack (most often via mobile devices) and the uploading of the video online[918]. Cyberbullying is not always and certainly not only a matter for data protection law. In particular, forms of cyberbullying are specifically regulated under criminal law in the framework of harassment, stalking, violence, violation of victim's honour, dignity, reputation, computer-related crimes (hacking, illegal access to data stored in a computer). In practice, the problem of cyberbullying is addressed using data protection law and authorities.[919]

Cyberbullying is not always and not only the matter of data protection law. Academics define cyberbullying underlining some of its specific elements, such as the use of electronic means, intentional harm, imbalance of power, repetition, sense of anonymity and lack of accountability.[920] Cyberbullying may have many different forms and only some of its forms coincide with data protection violations. These forms are fraping and impersonating (logging into the victims social networking account and impersonating him by posting inappropriate content), catfishing (stealing online identities, e.g. photos, and creating social networking profiles for deceptive purposes).[921] Another phenomenon of this type, ironically called as "happy slapping", refers to recording of a physical attack (most often via mobile devices) and uploading the video online[922]. In practice, the problem of cyberbullying is also addressed using data protection law and authorities.[923] Other forms of cyberbullying are regulated under criminal law in the framework of harassment, stalking, violence, violation of victim's honour, dignity, reputation, computer-related crimes (hacking, illegal access to data stored in a computer).

5.5.1.4. Harms to dignity and reputation

Harms to dignity and reputation include embarrassment, humiliation, etc. Harm to dignity and reputation might arise from violations of data protection law, e.g. publication of photos without individual's consent, but also from other crimes closely related to personal data disclosure such as defamation, cyberharassment, cyberbullying, online impersonation or revenge porn[924]. For example, disclosure of intimate personal habits, humiliating statements

[916] On the definition and regulation of cyberbullying see European Parliament, Cyberbullying among young people, Study for the LIBE Committee, 2016, available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

[917] Willard, 'Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social', (2007), 255-256.

[918] M. Palasinski, Turning assault into a "harmless prank"–teenage perspectives on happy slapping, Journal of Interpersonal Violence, 28 (9) (2013), pp. 1909-1923

[919] In Italy, the new Anti-bullying law (Legge 29 maggio 2017 n. 71) is enforced by the Italian data protection authority.

[920] European Parliament, Cyberbullying among young people, Study for the LIBE Committee, 2016,

[921] Willard, 'Cyberbullying and Cyberthreats: Responding to the Challenge of Online Social', (2007), 255-256.

[922] M. Palasinski, Turning assault into a "harmless prank"–teenage perspectives on happy slapping, Journal of Interpersonal Violence, 28 (9) (2013), pp. 1909-1923

[923] In Italy, the new Anti-bullying law (Legge 29 maggio 2017 n. 71) is enforced by the Italian data protection authority.

[924] Tiziana Cantone: Suicide following years of humiliation online stuns Italy," BBC News, 16 September 2016. Jorg Leijten, "ROC hoeft niet mee te werken aan onderzoek seksfilmpje," NRC, 21 September 2016. Paul Farrel, "Nude photos of Jennifer Lawrence and others posted online by alleged hacker," The Guardian, 1 September 2014.

or images to the public may cause embarrassment. Technological attack on a bullied person's blog (hacking into his or her accounts, sending offending messages in his or her name, or setting up a defamatory internet website to disseminate the victim's personal information or video clips without consent) harms the victim's dignity and reputation. Empirical research confirms the occurrence of violations related to personal data misuse on an individual level listing the hacking of social media accounts, creation of fake profiles, and impersonation as actual situation that upset children online.[925]

5.5.1.5. Societal or architectural harms

Societal hams may include the sense of being always observed resulting in a chilling effect or loss of creativity. Constant parental monitoring of children through location tracking apps may also have negative consequences including psychological problems. The continuous monitoring of children's location and conversations through the use of smartwatches might have potentially negative effects on children's development and create false sense of security.[926] The extensive "monitoring" function of some smartwatches (e.g., the Viksjord device/SeTracker app) can be seen as problematic as it not only enables one to listen to the conversations of children without their knowledge, but also to monitor anyone who is close to the child.[927] Permanent CCTV surveillance in classrooms can affect students' freedom of learning and of speech, thus also impacting their right to the development of a personality.[928] Even, the still "developing conception of their own freedom can become compromised" if children "assume from an early age that it is normal to be monitored".[929] Harms from profiling, such as stigmatisation, discrimination, could also be attributed to societal harms. Profiling can lead to surreptitious influence and customisation of individual behaviour[930], constraints to individual autonomy[931], unfair discriminatory decisions ("narrowed options and social discrimination")[932], power asymmetries and associated power inequalities[933].

5.5.2. Attributes of privacy harms

Two attributes should be considered for each harm. First, the victims of the harm which may belong to the following categories: 1) individual data subjects; 2) specific groups of data subjects based on age, gender, religion, ethnicity or interests/behaviour, etc. and 3) society. It is influenced by the scale attribute of the feared event. Individual child as a data subject might

---

[925] Giovanna Mascheroni, Kjartan Ólafsson, *Net children go mobile: risks and opportunities*, 2ed. Educatt, 2014.
[926] In Norway, the use of smartwatches for children has been criticized by the Ombudsman for Children and the Data Protection Authority, and Save the Children, available at: https://barneombudsbloggen.wordpress.com/2016/04/28/gps-sporing-av-barn-er-ikke-greit/ and at: https://www.nrk.no/livsstil/_-falsk-trygghet-a-spore-barna-med-gps-pa-skoleveien-1.13103688
[927] Forbrukerrådet, WatchOut: Analysis of smartwatches for children, October, 2017, availabel at: https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf
[928] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160, 11 February 2009, p. 16
[929] Ibid.
[930] M. Hildebrandt, Profiling and the Identity of the European Citizen. In: Hildebrandt M., Gutwirth S. (eds) Profiling the European Citizen. Springer, Dordrecht, 2008, p. 307.
[931] Ibid., p. 63.
[932] Joseph Turow, The Daily You*:* How the New Advertising Industry Is Defining Your Identity and Your Worth, New Haven, Yale University Press, 2011, p. 89.
[933] David Lyon, Surveillance Studies: An Overview. Oxford: Polity Press, 2007, p. 101.

be the victim of the harm when he is a single subject on which the harm is inflicted, for example his personal data is disclosed online and he is impersonated, etc. Children using a particular service or product can be profiled and targeted as a group infringing their group privacy. Recent class actions brought by consumer groups against intrusive data collection practices from children using connected toys [934] demonstrate how children can be victims as a specific group. Similarly, a class at a school could be affected as a defined group: video surveillance and constant monitoring at school might cause damage to the development of personality, construction of one's identity, autonomous action, group flourishing to the fullest extent.[935]

It is also important to consider various attributes of the data subject itself in a DPIA framework as these attributes have various effects on the rest of the analysis. Some useful attributes could be, for example, whether the data subject belongs to a vulnerable section of the society, such as children coming from disadvantaged families, children with psychological difficulties, and other factors. The societal context would also be important in deciding what constitutes a vulnerable section.

The second attribute is the intensity of a harm, which expresses the various effects of a harm on the victims. It depends on factors such as the duration of the harm or the extent of damage caused. It is also influenced by the irreversibility of the corresponding feared event, the stakeholder relationships and external factors such as societal norms. If a feared event has high irreversibility, then its impact on the victim is more intense than if it has low irreversibility. Similarly, weaker power positions of data subjects with respect to data controllers may make it more difficult for data subjects to have the harm stopped or addressed, thus increasing the intensity of the harm.

Privacy harms suffered by children are difficult to measure and the literature on this subject is sparse.[936] Harms that may result from internet use (online safety harms such as bullying, contact with strangers, exposure to pornography) more generally have been studied by the EU Kids Online project members, but privacy has not featured prominently in this research.[937] Some evidence, based on police, hospital, court and medical records, exists on actual harms when children are sexually abused and traumatised psychologically or physically after getting into contact with a perpetrator online.[938] Often, empirical surveys report "not the actual risk (i.e., the probability of harm to the child population) but the risk of the risk (the probability of something happening – commonly called 'online risk') that might result in harm; but whether it does, and for how many it does, remains unknown."[939] Yet, not all children who encountered online risks experience a harm. Important risk factors are "social psychological factors on the part of the child (such as facing psychological difficulties or having a tendency to sensation-seeking); as for protective factors, children's self-esteem and their parents' strategies for mediating the internet were shown to matter, though not in any simple fashion."[940]

---

[934] On group privacy see Linnet Taylor, Luciano Floridi, Bart van der Sloot (eds.), Group privacy: New Challenges of Data Technologies, Springer 2017.

[935] Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) WP 160, 11 February 2009, p. 16

[936] Vera Slavtcheva-Petkova, Victoria Jane Nash & Monica Bulger, Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research, Information, Communication & Society Vol. 18 , Iss. 1, 2015.

[937] Sonia Livingstone et al., 'Risks and safety on the Internet: The perspective of European children' (LSE, EU Kids Online, London 2011)

[938] Vera Slavtcheva-Petkova, Victoria Jane Nash & Monica Bulger, Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research, Information, Communication & Society Vol. 18 , Iss. 1, 2015.

[939] Sonia Livingstone, Online risk, harm and vulnerability: Reflections on the evidence base for child Internet safety policy, 2013, available at: http://www.ehu.eus/zer/hemeroteca/pdfs/zer35-01-livingstone.pdf p. 18

[940] Ibid.

Nevertheless, it could be claimed that the same harms may be more serious and have a more damaging impact on children than on adults. A child is a person who "has not yet achieved physical and psychological maturity" but is "in the process of developing physically and mentally to become an adult."[941] These two aspects makes him a particular victim of the harm. Harm can be caused to his harmonious development and growth, and the creation of a child's - still-developing – personality can be constrained. The importance of privacy for persons who have not yet reached physical, psychological and intellectual maturity has been explicitly underlined in case law relating to children's privacy, in several national courts around the world. In Germany, the Constitutional court explicitly recognised that children are 'persons-in-the-making' and they have a 'right to become [i.e., to freely develop into] a [full] person'[942]. As a consequence, children deserve *extra* protection in so far as the collection and disclosure of their personal data must be more rigorously justified than for adults whose personality is already-developed. Similarly, the Supreme Court of Canada also underlined the 'undoubted constitutional significance' of children's privacy and the special necessity to protect it. In its case law, the Court has recognised the 'inherent vulnerability of children' and their 'diminished moral culpability'. It has held that the privacy of children should be equally, if not more strongly protected, than that of adults, not only to avoid concrete harms, such as labelling and stigmatization, but, fundamentally, to guarantee the physical and moral autonomy and the well-being of the individual.[943] The French data protection authority (CNIL) equally described a child as someone who lacks psychological, intellectual and physical maturity, and who is still constructing his personality 'through a series of metamorphoses'.[944] Due to their personality being in development, law considers children to be in need of special protection against themselves (negative decisions that they themselves may take) and various risk sources.

Some harms may be irreversible for children as they can have a negative impact on child personality and development, i.e. the effect might last for the whole life. Also, the duration of the harm might be longer not only because it might take time to understand the harm but also for children it might be difficult to have the inflicted harm stopped due to their weaker position and lack of representation, lower understanding of the harm or technical and legal means to be used. For example, a personal data misuse (identity hacking) online on a massive scale could be difficult to stop due to slow or non-existing cooperation from the side of the internet service providers.[945] Practice shows that in some cases it can take more than one year to terminate the harm (to remove offensive posts, videos, pictures, to close fake profiles on social networking sites, to eliminate related results from search engines) and to mitigate the consequences, as the internet allows for personal data to be easily copied and replicated.[946] Re-emerging publication of personal data online can result into secondary victimisation and trigger negative psychological states in the victim.

---

[941] Ibid, p. 3.

[942] Case BVerfG, 1 BvR 1353/99 of 31.3.2000

[943] Case A.B. v. Bragg Communications Inc. 2012 SCC 46. [2012] 2 S.C.R. 567. Available at: http://canlii.ca/en/ca/scc/doc/2012/2012scc46/2012scc46.html

[944] CNIL, Internet et la collecte de données personnelles auprès des mineurs. (2001) Report. Available at: http://www.ac-grenoble.fr/juniors/droits/mineurs.pdf
See also Internet, les jeunes et la protection des données personnelles et de la vie privée. (2005) CNIL Fiche de Synthèse (summary).

[945] See e.g. A case of Freek, For more information (in Dutch) on the case can be found on Mijnkindonline website: http://mijnkindonline.nl/artikelen/hoe-%C3%A9%C3%A9n-gestolen-profielfoto-op-twitter-leidt-tot-een-wereldwijde-lastercampagne

[946] Ibid.

6. Conclusions

The paper proposed that data controllers processing personal data of children should consider carrying out child-specific rather than generic data protection impact assessments (DPIAs). Based on the PRIAM methodology, the paper discussed technical aspects of the child-tailored DPIA specifying its concrete components (personal data, risk sources, feared events, privacy weaknesses and privacy harms) and their attributes, and provided examples related to risks for children in the information society context. The proposed framework enables data controllers to address the particular needs and rights of children as data subjects.

Several questions are not fully addressed in this paper and require further research and analysis. More general questions include: whether and how child-specific DPIAs should be used by information society service providers offering mixed audience services; how the DPIA process should involve children as data subjects and take into account their views, and other broader questions related to the assessment of the necessity and proportionality of the processing. There is, further, a need for detailed research to develop harm trees to represent the relationship among the exploitation of privacy weaknesses by the risk sources, the feared events and the privacy harms in the context of children and to specify how data controllers should select a set of counter-measures that brings the risk level of all harms associated with the system below a given acceptable level.

Chapter 7

Protecting Children's Privacy Online: A Critical Look to Four European Self-regulatory Initiatives

Published in a peer-reviewed journal as:

Macenaite M., Protecting Children's Privacy Online: A Critical Look to Four European Self-regulatory Initiatives, European Journal of Law and Technology, 7 (2), 2016.

Abstract

This article examines the rise of self-regulatory initiatives as private governance mechanisms adopted by the Internet industry in the EU to protect children's privacy online. It analyses four specific initiatives and performs a formal self-regulatory process analysis focusing on procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors) aspects, in order to reflect on the strengths and shortcomings of the self-regulatory process. The analysis shows significant limitations of self-regulation in the area of online child safety, characterized by broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often inexistent sanctions. It is argued that sector-specific, institutionalized European codes of conduct, which disentangle protection of online safety and privacy as policy aims, could permit achieving better formulation, adoption and enforcement of voluntary rules, and thus better safeguard the privacy of children in the dynamic multi-jurisdictional, multi-stakeholder dominated online environment.

Keywords: children; European Union; online risks; privacy; self-regulation; soft law

I. Introduction and background

The area of children's privacy protection on the Internet has recently witnessed a vast increase in attention and regulation within the EU. There are several driving factors behind such developments. First, the importance of children rights, including the right to privacy and personal data protection, has grown. The EU has not only enshrined children's rights to protection and care in the European Charter of Fundamental Rights, but also has identified effective protection of these rights among the main priorities in its strategic documents (European Commission 2006, 2012). Second, a sharp increase in Internet usage by ever younger children and the complexity of the technology mediated environment has raised serious concerns about online child safety (Van der Hof, 2014). Protection of privacy and personal data in such a complex environment has become a prerequisite for guaranteeing online child safety and, thus, has started to constitute a separate, though interrelated, pillar within many online child safety initiatives. Third, since 1999 the European Commission's Safer

Internet Program has achieved remarkable progress in awareness raising and educational initiatives, multi-stakeholder involvement in safer Internet policy making and Internet content creation. Part of this Program fostered the gathering of more empirical data about online risks and their impact on children's online experiences across Europe (Livingston *et al.* 2012; O'Neill *et al.* 2013) which provided policy recommendations and implications (O'Neill *et al.* 2011). Empirical research has indicated that some of the most important concerns among children are related to personal data misuse and reputational damage, such as hacking of social media accounts, creation of fake profiles, and impersonation (Mascheroni & Ólafsson 2014). These concerns are well grounded, as 9% of children aged 11-16 have experienced personal data misuse online (Livingstone *at al*. 2011). Research has also clearly revealed the difficulties that children face when finding and using reporting tools and privacy settings to protect themselves online (Livingstone *at al*. 2012). All this in turn has penetrated discussions and has called for action among policy makers, academics and other stakeholders.

Since the very beginning, the protection of children online as a policy area in the EU has entailed an "unshakable commitment to self-regulation" (O'Neill*et al.* 2013, p. 15). [1] As paradoxical as it may seem, the implementation of protection of children's rights to privacy and personal data protection - both fundamental human rights - has to a large extent been playing into the hands of the industry in their online safety initiatives. As self-regulation and private rule-making has been put forward by the European Commission as a cornerstone of the regulatory process of online child protection, the effectiveness of the concrete self-regulatory rules becomes crucial in order to guarantee actual protection. Despite the obvious advantages proposed by soft law, such as the socio-technological expertise of the industry, innovation, reactive speed and reduced costs for the public bodies, in essence private rule-making, in particular where self-regulation is involved, is still often perceived as inherently feeble or ineffective regulation (Scott *et al.* 2011). Due to the lack of transparency, accountability coupled with ineffective enforcement, legal and media governance scholars question the results that self-regulation can provide, perceiving them as rather limited in practice (Latzer *et al.* 2013; Koops *et al.*2006; Bonnici 2008). Scholars within regulation studies (Scott *et al.* 2011) worry that self-regulation - as a community-based mode of private governing - raises legitimacy problems, due to its significant differences from the traditional democratic government model. If private regulation is more than technical implementation of authority, it is questionable to what extent it can advance a fair struggle between competing public and private interests (Scott 2012). In cases involving a public interest, such as the protection of vulnerable Internet users, there is a question whether self-regulatory initiatives can afford such protection to the same extent as serve the interests of the private sector (Livingstone 2011). This is particularly true for the area of online self-regulation which in general is known to "suffer from the perception that the individual's privacy rights are in the hands of those who have the most to gain from the processing of personal data" (Bennett 2004, p. 233). As a consequence, self-regulation may easily result in "self-service by the industry, with public interests being neglected vis-à-vis private interests" (Latzer *et al.* 2013, p. 375). It is not surprising, therefore, that in order to balance public and private goals in the self-regulatory process, in reality public actors often need to play a more active (co-regulator's) role. However, due to the many different forms that co-regulation may take, it does not necessarily ensure effective regulatory outcome either.

Despite the diversity of rules and their adoption processes, the Internet industry has, until now, managed on a European level to agree on four alternative regulatory initiatives that, among their other provisions, substantially deal with the protection of the online privacy of children. [2] These initiatives include: an arrangement among social networking service providers - the Safer Social Networking Principles for the EU; two documents adopted by broad industry Coalitions - ICT and CEO Coalitions; and a sectorial code of conduct adopted by direct marketing companies to regulate the use of personal data in their activities. Although different, these four initiatives all have amongst their other objectives the aim to mitigate online privacy risks, such as personal data misuse, commercial data exploitation, conduct and contact risks.

The aim of this paper is to examine the emergence of self-regulatory initiatives in the EU, aiming to address online privacy risks for children as governance mechanisms and explore their strengths and shortcomings. By analyzing the key provisions in four self-regulatory initiatives, the paper aims to perform a formal self-regulatory process analysis, rather than self-regulatory outcome analysis, focusing on procedural regulatory aspects. The analysis is based on the evaluation criteria that, according to regulatory scholars, must be present in self-regulatory regimes to consider them as effective and legitimate, i.e. procedural criteria (rule formulation, monitoring, enforcement) and organizational criteria (organizational structures, role of public actors).

The paper is structured as follows. The first section provides a short overview of the rise of self-regulation in order to protect children from risks in the Digital Single Market, discussing the main drivers and catalysts of such a rise. The second section describes the current self-regulatory regime for the online privacy protection of children, drawing on two different areas: online child safety and online advertising. Four self-regulatory initiatives are analyzed: the Safer Social Networking Principles, the CEO Coalition's Statement of Purpose, the ICT Coalition's Principles, and the FEDMA code. [3] These are the only existing self-regulatory initiatives dealing with online child privacy as a substantial part of their content. A formal self-regulatory process analysis focusing on the above-mentioned procedural and organizational aspects of the initiatives is performed in the third section, in order to evaluate their adequacy as regulatory mechanisms. The fourth section provides an evaluation of the initiatives. Conclusions are drawn in the last section.

1. The rise of self-regulation in the digital single market

Self-regulation related to the Internet has a long tradition. A wide range of voluntary initiatives, such as codes of conduct, rating/filtering systems, hotlines, standards, have been contributing to the protection of public interests and supplementing the existing state regulatory frameworks for two decades. One of the most prominent regulatory goals pursued by the means of self-regulation is the protection of minors in the communications sector, including on the Internet. In fact, reliance on self-regulation, rather than on legislation, in order to protect children's safety and privacy online in Europe can be traced back to the mid-1990s (European Commission 1996). Since then, policies aiming to create a safer - in more recent policy documents framed as "better" (European Commission 2012) - Internet for children place significant emphasis on

alternative regulatory initiatives, like self- and co-regulation (Lievens 2010). Preference for self-regulatory rule-making in relation to the online environment has been repeatedly confirmed in the main strategic EU policy documents, such as the Digital Agenda for Europe (COM/2010/0245 final), and the Agenda for Children's Rights (COM/2011/0060 final). References to sectorial industry codes of conduct were incorporated into the EU Data Protection Directive (95/46/EC), the EU Unfair Commercial Practices Directive (2005/29/EC) and, most recently, the General Data Protection Regulation (2016/679). All of these acts encourage self-regulation by the industry in general and, in the latter case, codes of conduct to protect the privacy and personal data of minors in particular.

There are various reasons why the EU considers industry self-regulation as the preferred option in the area of online child safety and privacy protection. More generally, a tendency to relate voluntary rule making rather than hard law with cyberspace regulation has been clearly expressed since the infancy of the Internet and grounded in cyber-libertarian ideas about an independent and unregulated cyberspace (Barlow 1996, Weber 2002). In fact, the Internet being global creates worldwide problems, such as safety and privacy risks for the users, which go beyond the capacity of individual states to solve, and thus requires global solutions. Self-regulation allows for detaching these solutions from the complex hard law Internet-related dilemmas of jurisdiction, applicable law and effective cross-border enforcement of legislation. It therefore also allows for softly reducing regulatory fragmentation on both sides of the Atlantic, getting US-based companies providing services to the EU citizens on board and imposing voluntary rules on them.

Other reasons that have driven the rise of self-regulation include the rapidly changing technological landscape and the difficulty of adjusting the national laws of the Member States to the new Internet-related developments (De Haan *et al.* 2013). Self-regulation was thus seen as able to address the emerging issues in a more time-saving and cost-efficient way. Also, multi-stakeholder involvement into the regulatory process and an informal-law-making environment seemed to promise more expertise and innovation than the traditional law making process and as a collective effort permitted reconciliation of conflicting interests - to preserve fundamental human values in the face of economic and technological pressures. In this respect, self-regulation was seen as able "to operationalize vague and general policy objectives" and provide practical guidance to the relevant parties on how to carry out their activities, in such a way "moving discussions from high-level policy rhetoric and slogans to more mundane, nitty-gritty action" (Webb 2004, pp.14-15). This evidenced a way to depoliticize important public issues, replacing them with technical solutions, procedures, and formalities driven by industry (Webb 2004). For instance, reliance on practical instruments such as parental control software, reporting mechanisms, content rating, and filtering systems introduced by self-regulation has allowed the EU to respect both freedom of expression and internal market and competition rules (Lievens 2010).

Finally, protection of online privacy in particular requires achieving a careful balance between ensuring the free flow of information and safeguarding the rights of users. Balancing these and similar competing interests can be complicated in legislative instruments not only due to their typical features such as rigidity or central implementation, but also the sensitivities involved.

For example, as regards Internet content regulation, there is a propensity for state censorship, and therefore regulation in this area can be intentionally left to private parties (Lievens 2010).

2. Self-regulatory initiatives addressing online child privacy

This section introduces the four EU self-regulatory initiatives adopted to mitigate online privacy risks for children, with the focus on their main characteristics (the year of the adoption, actors involved, nature and scope of the initiatives and the privacy-related provisions). All child-related provisions of the four initiatives are summarized and compared in Table 1 below.

2.1. Safer Social Networking Principles

The Safer Social Networking Principles for the EU (the SNS Principles) (European Commission 2009) is an early example of self-regulation in the area of online safety of minors. Initiated and supported by the European Commission, this self-regulatory initiative was adopted in 2009 and brings together approximately 20 social networking service (SNS) companies. The common goal of the participants, as claimed in the introductory part of the Principles, is "to maximise the benefits of the Internet while managing the potential risks to children and young people". To reach this goal, the providers have to assess the risk of potential harm that their service may cause to children, and consider the application of the specific seven overarching principles-guidelines. Two principles in particular encourage a safe approach towards personal information and privacy by having adequate safety tools and policies implemented in online social networking services. The third Principle requires empowering children through tools and technology and providing them with assistance with regard to inappropriate or unwanted content or conduct through special measures and technological tools. Concrete measures and tools that service providers should offer include, for example, non-searchable private profiles, profiles set to 'private' by default, ability to control who can access full profiles and post comments, 'easy-to-use' report tools. The sixth Principle asks service providers to enable and encourage their users to employ a safe approach to personal information and privacy through privacy settings and supporting information. Providers should offer user-friendly and accessible privacy options that enable users to make informed decisions about personal information that they publish and allow for privacy status and setting to be visible all the time. The remaining principles focus on awareness raising about online safety, age-appropriate services for the intended audience (e.g. indication of the minimum registration age, deletion of under-aged user accounts), and effective mechanisms to report inappropriate content and behaviour.

In essence, the SNS Principles provide only guidance for the providers of SNS and, thus, are merely aspirational in their nature. They are in no way prescriptive or legally binding. Participating SNS providers are left with a wide discretionary power while judging whether to respect certain principles and to what extent, considering the particular nature of their services. This leads to inconsistent and hardly measurable enforcement of the Principles, one of the shortcomings which will be discussed later in this paper.

2.2. Coalition to make a better and safer internet for children

In contrast to the SNS Principles, an initiative which aims to shape the behavior of private actors in a technology-specific domain, the Coalition to Make a Better and Safer Internet for Children (CEO Coalition), has been designed to gather a broad range of private companies working in various sectors of the ICT industry, such as operating system providers, handset manufacturers, Internet Service Providers, broadcasters, social networks and mobile operators. Launched in December 2011 on a high political level - personally by the Vice-President of the European Commission responsible for the Digital Agenda for Europe N. Kroes - the CEO Coalition aims to propose and develop, first of all, technical solutions and measures to protect children online. It was hoped that later these solutions proposed by the Coalition members can also be embraced by other market players. This initiative spans traditional technological or sectorial boundaries, and is defined by the practice in which companies are engaged - providing ICT services or products directed at or used by minors rather than by specific technology, like the SNS Principles.

Since its formation, around 31 companies have joined the CEO Coalition. According to the CEO Coalition's Statement of Purpose (CEO Coalition 2011), the five areas in which the companies agreed to take action and develop solutions include: tools for users to report harmful content and contact, age-appropriate privacy settings, content classification, parental controls, effective take down of child abuse material. The second area - age-appropriate privacy settings - is the most important reference to online privacy that can be found in the Coalition's Statement of Purpose. However, the intention of Coalition members in this area has been limited to pooling current practices and data together on a possible single appropriate level of privacy settings across services and related user information protocols. The mere compilation of a database on these issues seems to be a very modest aim, acknowledging privacy as a human right and the influence of default-settings on the online behavior and practices of children. The lack of ambitious and clear goals has characterized this initiative since its inception and consequently attracted criticism from various actors within civil society (EDRi 2013).

Despite the initial enthusiasm, especially on the political level, currently the CEO Coalition is not very active in practice. After the first year of functioning the progress has been suspended, although publicly the Coalition members and the European Commission affirmed their commitments to collaborate. Apart from a few spin-offs from the Coalition in the area of content classification, future collaboration (if it happens at all) appears to be essentially limited to awareness raising and the sharing of best practices and educational materials among the Coalition members.

2.3. ICT coalition for children online

Another self-regulatory initiative that is similar to the CEO Coalition in terms of content, membership and timing is the ICT Coalition for Children Online (ICT Coalition). The main difference between the two initiatives lies in their formation process. The ICT Coalition was formed by the industry without any involvement of the European Commission. In its own capacity, it elaborated a set of principles - Principles for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU (ICT Coalition 2012). Although adopted a month after the CEO Coalition's Statement of Purpose, in January 2012, the ICT

Principles actually preceded the CEO Coalition in terms of negotiations and drafting by one year. Almost identically to the CEO Coalition, the ICT Coalition Principles pursues the aim "to help younger Internet users across Europe to make the most of the online world and deal with any potential challenges and risks" [4]. Given the overlap in focus and members, it is not entirely clear why the CEO Coalition was initiated in the first place, creating a parallel initiative to the already ongoing industry effort.

The ICT Coalition is made up of 23 different companies from across the ICT sector, and just as the CEO Coalition can be considered a functional initiative in its nature. In terms of scope, the ICT Coalition Principles focus on six key areas: harmful content, parental controls, abuse/misuse of technology, sexual abuse content/illegal contact, digital literacy and awareness, and privacy. The privacy area is defined by Principle 5, according to which companies promise to manage and provide options for privacy settings in a user friendly way (easy to understand, prominently placed, user friendly and accessible) and enable children and parents to make informed decisions, as well as to raise awareness among all relevant parties. This commitment, if still limited in its aim, provides much more clear and ambitious goal than the action of the CEO Coalition on the same matter.

In practice, the ICT Principles oblige each company (or group of companies) to present a document, which states objectives to be attained and benchmarks as far as applicable to its specific services and products, which would allow proper monitoring of further implementation in the six areas mentioned above. Companies that are signatories to this initiative are expected to report on their progress after the adoption of the Principles. More than half of the companies have published their progress reports on the Coalition's websites, based on which an independent review of the achievements took place.

2.4. European code of practice for the use of personal data in direct marketing

A very different initiative in its nature compared to the three online child safety initiatives is the European Code of Practice for the Use of Personal Data in Direct Marketing (the Code) (FEDMA 2003), a self-regulatory initiative adopted in the advertising sector to regulate data collection for marketing purposes. The aim of the Code is, in part, to protect minors from commercial risks inherent to the online world. The Code is based on more detailed and thorough analysis of how industry collects and processes personal information rather than broad commitments and statements.

The Code was adopted in 2003 by the Federation for European Direct and Interactive Marketing (FEDMA), a sectorial organization widely representing the direct and online marketing industry on the European level through promotion and protection of its interests, lobbying for a favorable legislative environment and education and training. Currently FEDMA reports to have around 400 direct members in more than 30 countries, and nearly 10,000 companies are represented indirectly through their membership in national Direct Marketing Associations. The Code has been implemented on the national level by all FEDMA members.

The Code is European in character, as the Article 29 Working Party, a European body representing the national data protection authorities, has approved it in accordance with Directive 95/46/EC as providing sufficient added value by addressing data protection problems in the direct marketing sector (A29WP 2003). By approving the Code, the Article 29 Working Party also underlined that the general provisions of the Code cannot solve all specific issues related to online direct marketing, and asked FEDMA to draft an annex to the Code applicable to the online environment and in particular addressing the protection of children. As a result, in 2010 following an extensive and long consultation process with the Article 29 Working Party, the Code has been supplemented with an Annex applicable to online marketing (FEDMA 2010), which was also approved by the Article 29 Data Protection Working Party (A29 WP 2010). Section 6 of the Annex deals with the protection of children and, among other things, establishes the responsibility of the data controller for setting up the procedures to guarantee verification of the age of the minor and the authenticity of the parental consent. However, it acknowledges that there is no easily accessible, universally accepted age verification system available on the Internet. The Code also obliges data controllers to provide child-appropriate information about data processing, prohibits family data collection from children, limits collection of sensitive data, and forbids incentives to provide personal data for marketing purposes or in exchange for a reward, including games of chance, tombola or lotteries.

Table 1. Child-related provisions of the four initiatives

Provisions	SNS PRINCIPLES	CEO STATEMENT	ICT PRINCIPLES	FEDMA CODE
Awareness raising, user empowerment	✓	-	✓	-
Age appropriate services	✓	-	-	-
Conduct & content reporting tools	✓	✓	✓	-
User-friendly privacy settings	✓	✓	✓	-
Content classification	-	✓	✓	-
Parental controls	✓	✓	✓	-
Take down of illegal content	✓	✓	✓	-
Age verification	-	-	-	✓
Understandable information	✓	-	✓	✓
Prohibition to collect information about family members	-	-	-	✓
Requirement of prior consent for collection of sensitive data	-	-	-	✓
Prohibition to incentivize children to provide personal data in exchange for rewards	-	-	-	✓

3. Comparative assessment of the self-regulatory initiatives

The comparative assessment in this section is based on the main evaluation criteria that, according to scholars in the areas of electronic communication and technology regulation and

governance, must be present in self-regulatory regimes to consider them as effective and legitimate.

Although in the electronic communications sector conceptual frameworks for evaluation of self- and co- regulatory initiatives are still in the initial stage of their development (Latzer *et al.* 2013), several efforts to propose a set of criteria to evaluate the effectiveness of voluntary rules have been made by academics (Schulz and Held, 2002; Latzer *et al.* 2007; 2013). On a policy level, the European Commission has also recently looked for criteria to define accountable and efficient self-regulation which could deliver on its societal goals (CoP 2013). These contributions highlight the need for clearly formulated rules and requirements, effective monitoring and oversight, enforcement mechanisms and sanctions, including independent complaint assessment procedure. Writings on self-regulation in industries other than ICT have similar requirements for effective industry self-regulatory arrangements (Bowman & Hodge 2009; Sethi and Emelianova 2006; Gunningham & Rees 1997; Doing & Wilson 1998; Jenkins 2001).

In addition, interdisciplinary literature on governance and self-regulation underlines the importance of a background presence of public actors (Ayres & Braithwaite 1992, Gunningham & Grabosky 1998, Rees 1997) and the existence of recognized industry organizations (Latzer *et al.* 2007) in enhancing the adoption and enforcement capacity of self-regulatory rules. The latter refers to acknowledged and structured industry bodies, such as the associations of specific industry segments, which have experience and administrative capacity in dealing with self-regulation.

Taking into account the contributions mentioned above, the paper uses two sets of criteria to evaluate the self-regulatory process related to the initiatives described earlier: procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors). These criteria and their precise indicators are applied to the four initiatives in Table 2.

3.1. Content of the rules

Clearly defined objectives and measurable standards set forth by self-regulation that are able to add additional value to the existing legislative provisions can enhance potential advantages and reduce failures of self-regulation. As noted by Latzer *et al.* (2007), the way the self- and co-regulatory initiatives are designed may constitute an important enabling institutional/organizational factor. Ideally, a self-regulatory initiative should specify a mission statement with a reference to a public policy objective, define clear, measurable goals and intended outcomes. Additionally, it should clarify the regulatory added value in relation to the existing state regulation (Latzer *et al.* 2007).

When comparing the four initiatives, one of the most striking differences lies in the formulation of the rules embodied in the self-regulatory texts under analysis. All the initiatives adopted in the online child safety domain set only general targets and aims, which can be denoted more as intentions or statements of commitments rather than as rules. Consequently, they add little

to the existing legislative framework. The CEO Coalition's Statement of Purpose and reports provide the clearest illustration of broad objectives from all three safety-related initiatives (e.g. "to take positive action to make the Internet a better place for kids"; to "continue to work with wider stakeholders to raise awareness on parental controls"). These statements also almost entirely repeat the legislative requirements ("to offer clear and understandable information" in privacy policies). In contrast, the sectorial code in the online advertising area provides much more precise rules and obligations for its members. [5] It is thus a much more measurable self-regulatory text which builds upon the general data protection standards that are not tailored to children, an additional level of specific protection adding value to the existing data protection law. For example, the FEDMA members are required to obtain prior consent before collecting sensitive data or are prohibited from processing certain types of data.

Lack of clear, prescriptive rules and measurable standards in the policy area of child online safety leads to several shortcomings. First, companies adhere to the same initiative in very different ways. Some of the companies commit to do very little, some take obligations seriously within the scope of the same principles and others even claim that certain obligations are not applicable to their services or products. Second, due to imprecise goals it is difficult to measure and compare compliance among the members and to evaluate the level of fulfillment of the agreed objectives. The latter problem will be discussed in more detail below.

Notwithstanding this, one should note that broad and vague objectives do not automatically lead to the failure of a self-regulatory initiative. Vague prescriptions and high-level statements of intent not only allow for adapting the requirements to specific services and products, but also leave companies room for innovative solutions. In addition, the inclusion of more prescriptive rules may be premature in the beginning of the self-regulatory process, especially in the areas where technological solutions are still scarce, like in relation to age verification technologies. This, however, does not preclude the possibility of developing quantifiable and enforceable standards over time.

In addition, from a policy making perspective it may be questioned whether companies would be at all willing to commit themselves to something more than broad statements and intentions. Even if the state of the art of technological developments and expertise of the industry may theoretically allow for prescriptive provisions, the motivation to have detailed self-regulatory rules can still depend on various other factors. These factors, for instance, can be pressure on corporate image (Gunningham 1995) or peer pressure and mutual benefits, the perception of the importance of avoiding hard regulation, the willingness to forestall or shape future laws, and the existence of distrustful public attitudes towards their services or technology (Webb & Morrison 2004, Bowman & Hodge 2009). Moreover, the motivation of companies also can be largely profit-oriented in nature, such as increasing or maintaining customers, decreasing risk, or decreasing the likelihood of a legal violation and liability (Webb 2004). As direct economic benefit for the industry in the policy area of online child protection is clearly not a driving force to create or join self-regulatory initiatives, broad and vague commitments should be of no surprise.

3.2. Monitoring and oversight

There is wide support for the view that effective self-regulation requires independent or third-party monitoring and oversight (Schulz and Held 2002; CoP 2013, Latzer *et al.* 2007; 2013). Drawing upon the experiences of self-regulation in industries other than ICT, independent monitoring and compliance verification appears to be an important precondition for any effective industry self-regulatory arrangement (Bowman & Hodge 2009; Sethi and Emelianova 2006). No less important is the "willingness to make the findings of the independent external audit available to the public without prior censorship" (Sethi and Emelianova 2006, p. 230-231). Other scholars have similarly claimed that monitoring and disclosure clearly matters (Gunningham & Rees 1997; Doing & Wilson 1998; Jenkins 2001). Jenkins (2001, p. iv), in an analysis of corporate codes of conduct, recognized that it is essential to include provisions on effective monitoring into them in order to see an impact and, in addition, claimed that "the reluctance of many firms to include independent monitoring as an integral part of their code gives rise to some suspicion that they may be used as a public relations exercise rather than a genuine attempt at improving conditions and performance" (Jenkins 2001, p. 27).

Different oversight and monitoring mechanisms are used by each of the initiatives, ranging from external oversight to a pure information disclosure practice and self-reporting. Two of the initiatives, the SNS Principles and the ICT Principles, enjoy the strongest evaluation procedures carried out by independent third parties. Compliance with the SNS Principles is periodically measured through the evaluations carried out by external experts. However, their final reports are approved and published by the European Commission, causing doubts about the total independence of the conclusions. Since the adoption of the initiatives, two such evaluations have taken place (Staksrud & Lobe 2010; Donoso 2011). The evaluations were carried out in two steps: assessment of individual self-declarations of the participating SNS and practical testing of their websites. Overall, according to the latest assessment in 2011, only 3 from 14 self-declarations were assessed as "very satisfactory", while the remaining 9 were only "rather satisfactory" and 2 "unsatisfactory" (Donoso 2011). Self-declarations were better evaluated than their real implementation on the concrete websites, underlining the problem of objectiveness among participating SNS. Although the evaluation of other principles showed some signs of success, privacy was shown to be the area where the majority of the SNS failed to meet their commitments. Only 3 SNS from 14 providers were evaluated as very satisfactory. The main weakness noted by the assessor related to the lack of explicit information regarding the characteristics (e.g. age-appropriateness, availability, user- friendliness, etc.) of the privacy settings on the services and the lack of information regarding whether these services provide users with supporting information to help them make informed decisions about their privacy settings.

Yet, even positive evaluation does not necessarily reflect the practical impact that self-regulation has on Internet users. Although the majority of the tested SNS demonstrated some positive progress, tangible results, especially in the area of privacy protection, remain limited. As indicated by empirical evidence-based research, which compared SNS Principles with 9-16-year-old children's experiences and skills on the social networks, many industry players do not meet their commitments (e.g. in guaranteeing effective age-restriction or setting children's profiles to 'private') (Livingstone *et al.* 2013).

Similarly to the SNS Principles, the ICT Coalition has lately introduced an independent monitoring mechanism to evaluate how the Coalition members implement the ICT Principles. It established a position of an independent assessor who carried out his first assessment in 2014 (O'Neill 2014). The evaluation was based on the statements of the ICT Coalition members, without actual testing of their services and products. Although individual commitments and best practices in the six broad areas related to online safety are to be applauded, the concrete implementation and measurement of compliance may be questioned. Given the above-mentioned trend among the SNS providers to self-declare more than is actually implemented, only formal evaluation of declarations without comparing them with the actual achievements may have an impact on objective assessment results. Moreover, due to the broad, and sometimes ambiguous, targets, it is not clear from the assessment to what extent (and if at all) all the members of the ICT Coalition achieved the agreed goals. The report, therefore, looks more like a summary of best practices rather than an assessment indicating the actual level of compliance.

Contrary to the external evaluation schemes mentioned above, which admittedly have their shortcomings, it is much more difficult to establish compliance in the case of the CEO Coalition. It does not undergo any formal monitoring process, despite its own evaluation of the work in progress. Such self-assessment took place after the first year of functioning of the CEO Coalition and was rather broad, recognizing that progress had been made in all the working areas but more effort was needed to achieve the agreed goals (CEO Coalition 2012). In February 2013, the CEO Coalition published its final report containing recommendations and best practice description (CEO Coalition 2013). In addition, in January 2014 individual companies produced separate reports on how they have implemented or will implement the recommendations of the Coalition (CEO Coalition 2014). Such a self-evaluation mechanism appears to be very subjective and limited.

In contrast, the FEDMA Code sets forth a well-defined and institutionalized monitoring mechanism. According to the Code, the burden of monitoring has been primarily shifted to the national direct marketing associations (DMAs). It is not surprising, as advertising, even if it is a cross-border phenomenon, is also "very often nationally distinctive, using the local language, characters, and humor familiar to the target audience" (Verbruggen 2013, p. 515). Therefore, a national rather than European system of adoption, review and enforcement seem to better serve the goal of voluntary governance. In practice, several of the DMAs have a compliance tool in place and carry out compliance monitoring, either when a company becomes a new member of the national association with subsequently action only on complaints, or involving monitoring the compliance with the Code on a more regular basis (Fiquet M 2015, personal communication). For example, some of the DMAs have a certification program every year or every two years (Fiquet M 2015, personal communication). In addition, the Code encourages the companies themselves to regularly monitor how they conform to the provisions of the Code (for example, via self-audits), but this is more a piece of advice rather than a strict obligation. In addition to the main enforcement efforts on the national level, a "Data Protection Committee" has been established on the European level at FEDMA to monitor the application of the Code, to consider annually if a revision of the Code is necessary and to provide the Article 29 Working Party with an annual report on the functioning of the code at national level and in cross-border activities. However, despite the established internal structures and the

formal obligation to report to the national data protection authorities, the European Commission and the European Data Protection Supervisor (via the Article 29 Working Party meetings), FEDMA does not officially assess the extent to which its members comply with the code. Only some informal discussions on the functioning of the Code took place with the European Commission after the Code and the Annex were adopted (Fiquet M 2015, personal communication).

Lack of an independent monitoring scheme in the activities of the CEO Coalition can be seen as a very serious shortcoming. However, even if the remaining online safety initiatives are monitored and evaluated by independent experts, there are significant pitfalls: the final reports published by the European Commission may not be entirely independent, evaluation results may greatly depend on the methodology and sources used (actual testing of the services or evolution of self-declarations), and due to vague targets lack of a clear indication of the level of compliance. Also, the positive evaluation does not necessarily reflect the practical impact of self-regulation as, from the perspective of Internet users, empirical evidence may suggest that in reality companies fail to meet their commitments.

3.3. Enforcement

Enforcement of self-regulatory rules depends on the existence of and access to the procedures to handle possible complaints in relation to the infringement of the self-regulatory rules and the sanctioning of the members for established violations. Latzer *et al.* (2007, p. 21) identified the following elements of an adequate enforcement mechanism in relation to disputes and complaints: existence of a relevant enforcement organizational structure such as a unit to handle complaints, a defined enforcement and complaint handling procedure, a visible and well-known contact point to which to report potential infringements, an appropriate appeals mechanism. They claim that the level of enforcement can be measured based on the amount of complaints filed and disputes registered or any other modes of industry notice to members. Once a violation is found, a test of self-regulation effectiveness is "whether it has 'shown its teeth' to a member through some type of sanction" (Cave *et al.* 2008, p. 23), such as withdrawal of membership, or censure for non-compliance. The two elements of enforcement (i.e. complaint handling procedures and sanctioning mechanisms) will be analysed below.

Complaint handling procedures are not present in the majority of initiatives (the SNS Principles, the CEO and ICT Coalitions), with the exception of the FEDMA Code. The latter, being a European initiative, dedicates the establishment of procedures to solve any complaints that may arise from the application of the Code to the national DMAs. According to the information provided by FEDMA, the Code enforcement mechanisms have been put into practice and national DMAs have received and solved several complaints in cases of malpractice (Fiquet M 2015, personal communication). As set out in the officially established mechanisms, the complaints are normally handled by special compliance boards, ethic committees or similar commissions formed at the DMA level. Only if the DMAs appear to be unable to solve complaints due to their cross-border aspects, FEDMA could take up and investigate the dispute itself. The Code establishes a mechanism for that by stating that the investigation on the FEDMA level should be carried out by the Data Protection Committee, an

internal body composed of representatives from national direct marketing associations, FEDMA and companies that are direct FEDMA members according to its internal rules of procedure. In practice, however, up to now FEDMA has not yet received or handled any cross-border complaints (Fiquet M 2015, personal communication). The small number of actual complaints may well be related not so much to procedural enforcement issues, but to practical difficulties for individuals in complaining about online behavioral advertising. Online advertising substantially differs from traditional print, broadcast or outdoor advertising (Verbruggen 2014). As "advertisements may appear only to individual consumers and perhaps only once, it can be difficult to prove that the ad was served and that it violated the applicable code(s) of conduct" (Verbruggen 2014, p. 97).

Neither the SNS Principles nor the CEO Coalition self-regulatory initiatives include any reference to sanctions. As a result, only symbolic sanctioning mechanisms relating to companies' reputation can be used in order to improve compliance. In cases of poor performance, the European Commission in practice tends to put pressure on companies through "naming and shaming" in public press releases. [6] In contrast, an explicit reference to sanctions is present in the FEDMA code and shortly mentioned in the ICT Principles. Pursuant to the Code, as national DMAs are responsible for the application of the Code, they have to apply the same sanctions stipulated in their countries for the breaching of their national codes. Most of the time the sanctions applied by the DMAs on the national level include "naming and shaming", DMA membership removal or passing the complaint to the national regulators, such as the national data protection supervisory authorities (Fiquet M 2015, personal communication). Moreover, depending on the type of violation, if the FEDMA Data Protection Committee gets to handle the complaint - which, as mentioned earlier, has not been the case until now - it can equally recommend the FEDMA Board to expel a member or apply other sanctions (e.g. “to initiate legal action against a member or a non-member in order to safeguard the ethics of the profession”) (FEDMA 2003, p. 18). However, FEDMA is not able to enforce fines or apply other monetary sanctions due to the fact that it is a voluntary, fee-based membership organization and fines would diminish incentives for membership. To a lesser extent, a similar sanctioning possibility is present in the ICT Principles. The text of the Principles establishes a possibility to exclude a member, if it does not seek to apply the Principles. However, given the embryonic nature of the initiative, it is still not possible to know the extent to which the ICT Coalition will take this possibility seriously. In addition, contrary to the whole package of benefits that industry associations provide to its members (e.g. lobbying, good practice developments), exclusion from a Coalition does not seem to promise the same loss for companies and therefore calls into question the extent of the threatening power it may carry.

The absence of enforcement mechanisms and dissuasive sanctions in case of malpractice, and the lack of specific bodies to enforce them in the majority of the online child safety initiatives, present significant limitations. Reliance on symbolic sanctioning through public 'naming and shaming' does not help much to deal with violators or free riders. Sectorial industry associations, in contrast, tend to operate within a well-defined set of regulatory institutions and rules, which in turn provide for cohesive and appropriate organizational and sanctioning mechanisms for the implementation of self-regulatory rules. In addition, due to additional

benefits besides being part of the voluntary rule-making process, industry associations have a much wider impact on their members if they impose exclusions as a sanctioning mechanism.

3.4. Organizational structure of the industry

The availability of recognized organizations and their internal structures, such as secretariats and special committees, for regulatory tasks in the existing market environment may help to achieve a greater level of adoption and more effective implementation of self-regulatory rules. If a well-established organization in a particular segment can perform regulatory tasks and provide necessary organizational assistance, i.e. backup the initiatives, the practicability of adoption and compliance with voluntary schemes is much higher (Latzer *et al.* 2007). A significant difference exists between the FEDMA as a representative of a direct marketing industry and the other remaining multi-stakeholder dominated institutions in terms of their organization. FEDMA and the DMAs already have refined institutions, have experience with codes of conduct, and have necessary personnel and organizational structures that can monitor implementation, handle complaints, and impose fines. The need for a particular organizational structure seems to be increasingly recognized, but still under development, in the ICT Coalition, which has appointed an independent evaluator, hired an external consultant, and sought transparent and open functioning processes (creating a website, providing information to relevant stakeholders, etc.). The remaining online child safety initiatives are characterized by loose bonds among their members, and operate more as cooperative and consensual technical networks rather than structured organizations. Such open governing structures, what regulatory scholars (Kohler-Koch 2002; Kooiman 2003; March 1998, and Rhodes 1997) would call governance networks, are issue-specific constituencies build by a public authority as an activator, which interact though multilateral negotiations in order to upgrade common interests while pursuing the individual benefit (Kohler-Koch 2002). This model brings its own disadvantages of loss of oversight and steering and fragmented coordination.

The absence of the proper organizational structures in the online child safety initiatives, and reliance on the European Commission in terms of organizational matters, may be seen as negatively influencing their performance. Yet, as Weber (2012, p. 3) reminds us, "cyberspace is not regulated or supervised by any of the existing bodies" and "there is a certain lack of sufficiently involved international organisations". Apart from industrial associations for specific sectors, there are no stable organizational structures for ICT policy domains where multi-sectoral and multi-stakeholder action to protect vulnerable users is required. When the focus of regulation is child safety and privacy risks in conjunction, only a combination of different stakeholders representing a wide range of online technologies, services, platforms and business models can propose solutions.

3.5. Role of public actors

Potential intervention via hard-law by national or European authorities is considered to be an additional incentive for companies to adopt and enforce self-regulatory rules. The ability to

pose a real regulatory threat of intervention by public bodies can enable better adoption and enforcement of self-regulation (Latzer *et al.* 2007). In addition to providing the shadow of hierarchy, i.e. threatening to adopt legislation unless private actors accommodate the legislators' demands in self-regulatory rules, public bodies can actually be involved in the adoption and implementation of self-regulation. Although self-regulatory rules related to public interest could hardly be adopted without any kind of involvement from public institutions, possible forms of such involvement greatly differ. The possible levels of institutional involvement range from encouragement (provision of carrots, inspiration) and appreciation on a political level to financial and personnel support, collaboration on an institutional level, or even co-regulation (direct control in a legal sense), periodic reviews performed by public officials, establishment of alternative scenarios in case of failure (sticks), and a clear definition of responsibility among industry and public authorities (Latzer *et al.* 2007).

The EU institutions have never publicly threatened the industry with real and immediate legal provisions on child safety if self-regulation fails to deliver expected results. Several areas, however, like personal data protection and behavioral advertising, have been touched upon or are under consideration by the European Commission. The recent revision of the European Data Protection Directive (96/46/EC) has given a possibility to address protection of children's privacy online. The newly adopted General Data Protection Regulation (2016/679) has, for the first time, explicitly recognized that children deserve specific protection of their personal data, as "they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data" (Recital 38). The Regulation has introduced far-reaching changes in relation to the processing of children's personal data: it requires verifiable parental consent before processing personal data of children under the age of 16 (unless the Member States choose another age limit between 13 and 16), obliges companies to give information to children in a clear, audience-appropriate language, and foresees other additional rights and safeguards, such as the right to be forgotten. These legislative developments happened despite the fact that public consultation revealed the willingness of companies to develop codes of conduct together with the Article 29 Working Party and to ensure their proper enforcement rather than to have legislative provisions on child-related data protection matters (European Commission 2010). The actual influence of these new legislative provisions will, however, depend on how much practical guidance and specification the European Commission and data protection authorities will provide to companies implementing the General Data Protection Regulation.

Regarding the advertising sector, the "regulatory gorilla in the closet" (Verbruggen 2013) has been present for longer and felt more clearly. Children have been protected from Internet-based audiovisual services, programmes and advertisements as vulnerable consumers in the Directive 2010/13/EU on Audiovisual Media Services. Also, the European Commission is currently gathering evidence to explore whether the existing regulation is effective and adequate to protect children from online marketing in social media, online games and mobile applications, or whether changes are necessary in regulatory approach, including the initiatives taken by the industry (European Commission 2015). Based on the outcome of the exploration, potential amendments can be expected in relation to children as vulnerable consumers protected in the Guidance document to the Directive 2005/29/EC on Unfair Commercial Practices (SEC(2009) 1666) and to the upcoming review of the Directive on Audiovisual Media Services. It is

difficult to establish any connection between the legislative initiatives mentioned above and the better performance of the self-regulation under analysis.

As mentioned above, an adequate level of support from the public institutions is considered to significantly enhance the performance of self-regulatory initiatives. In fact, it is often claimed that co-regulation is the most successful form of self-regulation. In the area under analysis, the EU is the most intensively involved in the SNS Principles and the CEO Coalition, but mainly in the form of inspiration and financial and personnel support. The SNS Principles are financed under the EU Safer Internet Programme and the European Commission provides supporting activities, hosts industry and stakeholder meetings, hires independent experts for periodic assessments, publishes assessment results on its website and evaluates the compliance via press releases. Similarly, the CEO Coalition has been initiated by the Commissioner N. Kroes in person, inviting specific companies to participate in the initiative. In addition, the EU supports the work of the CEO Coalition on financial, know-how (Commission representatives participate in Coalition meetings) and organizational levels (hosts stakeholder meetings, publishes information on its website). Yet, as emphasized earlier, the rules of both initiatives are broad and rely more on good-will commitments rather than enforceable obligations resulting in limited added value to actual protection.

It therefore seems that content approval is more important for initiatives than procedural and political support, which may guarantee that industry takes on board all the most relevant public policy issues and challenges - in other words avoiding pick and choose tactics - as well as formulating clear and enforceable rules. In this respect, contrary to the SNS Principles and the CEO Coalition, the FEDMA code seems to experience a more balanced support from the public authorities. Although initiated entirely by the direct and online marketing industry, the European Commission together with the Article 29 Working Party has been closely involved in the drafting procedure of the Code. The rules on the protection of children are the direct result of such involvement as the Annex had been approved as compliant with and adding value to the EU data protection rules only after the provisions of child protection had been introduced.

As a result, the approval of self-regulatory rules as a procedural step in order to adopt a European code of conduct is not only a desired "political backing" of the self-regulatory rules for the industry but also a guarantee for those to be protected that their interests and societal values will be taken into account.

Table 2. Assessment of the four initiatives

Criteria		***SNS Principles***	***CEO Statement***	***ICT Principles***	***FEDMA Code***
Content of the rules	Prescriptive, measurable rules	-	-	-	✓
	Broad statements of intent	✓	✓	✓	-
Monitoring & oversight	Internal self-assessment	✓	✓	✓	✓
	External assessment by an independent party	✓	-	✓	-
Enforcement (complaints & sanctions)	Existence of a body to handle complaints	-	-	-	✓
	Defined complaint handling procedure	-	-	-	✓
	Reputational sanctions	✓	✓	✓	✓
	Organizational sanctions (expulsion, membership suspension)	-	-	✓	✓
Organisational structure	Industry association	-	-	-	✓
	Ad-hoc network/coalition	✓	✓	✓	-
Role of public actors	Initiator	✓	✓	-	-
	Approver	-	-	-	✓

4. The way forward

This analysis showed significant limitations of self-regulation in the online child safety area, characterized by broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often inexistent sanctions compared to a sector specific, institutionalized European code of conduct in the area of advertising.

Drawing on the differences in the online child safety and advertising domains, it seems that the policy goal of protecting children's privacy online can be approached from two different angles. Privacy can be viewed from a social or informational lens. The online child safety initiatives are mainly concerned with social privacy, a concept often used by the American scholars to note "the ability to control the social situation by navigating complex contextual cues, technical affordances, and social dynamics" (boyd 2014, p. 60) in the networked publics. It refers more to the negotiation of social boundaries, in particular to the management of diverse audiences through privacy settings and controls, and is entangled with online safety. The concept of social privacy and the risks to it relate to various values to be protected that are at stake, such as seclusion, intimacy, identity, reserve, self-determination and autonomy. Social privacy, being

about control of social situation and context (e.g. hiding from public environments), is a broad concept and significantly differs from informational privacy, which refers just to the control of the flow of personal data (Westin 1967). Informational privacy, a more European concept, and even more precisely protection of personal data from illegal and illegitimate collection and use, instead, is the focus of the sectoral - and not surprisingly European in its nature - FEDMA Code. While dealing with informational privacy in terms of personal data protection, a single risk and one well-defined facet of privacy, the rules and requirements for legitimate data processing are very clearly set in a legislative framework and, therefore, can be easily implemented also on a voluntary level. As a result, while addressing social privacy, with its inherently different safety and privacy risks on the Internet, in one initiative, the multi-scope online child safety initiatives unavoidably use deliberately vague language, leaving the companies to decide for themselves how they will respect each of the agreed requirements. It would be very difficult, if not impossible, to address all the aspects of social privacy in a uniform and measurable way. Consequently, clear and detailed rule-making is only possible when the rules aim to mitigate a single informational privacy risk, such as personal data misuse, in the sectorial code of the advertising industry. As a result, without denying the need for general rules to protect other aspects of privacy, it would be more beneficial to self-regulate online child privacy issues separately from safety initiatives and use sectorial industry associations for such self-regulatory tasks.

Such a human rights-based approach, instead of a safety-based approach, would consequently require the EU to take a stronger and better defined self-regulatory strategy. The conditions for that seem to be envisioned in the General Data Protection Regulation. It encourages associations and other bodies to prepare codes of conduct for the purpose of specifying the application of data protection provisions when the personal information is collected from children. The Regulation also requires an independent body which has an appropriate level of expertise and is accredited by the competent supervisory authority, to monitor compliance with codes of conduct. More reliance on sectorial codes would not only bring online privacy protection mechanisms more in line with the human rights perspective, but also possibly lead to clear rules given the possibility for public authorities to approve their content and the similarity of the industry players. As noted by Bennet (2004, p. 232), the main defining feature of the industry associations and their codes is "a broad consonance of economic interest and function, and by extension a similarity in the kinds of personal information collected and processed", and "sectoral codes permit, therefore, a more refined set of rules tailored to the issues within each industry".

The aim of the online child safety initiatives to empower the users through technological solutions to manage their social privacy could, instead, be partially realized by putting more pressure on the industry providing online services for children to implement the privacy by design and privacy by default principles. Special privacy protection tools should be implemented at the early design stage of online services and products offered to children and enabled by default. For example, services and applications could be designed in a way that only the minimum amount of personal data necessary to deliver the services are collected from children, and children are not subject to online behavioural targeting, including profiling. Privacy settings and reporting tools could be prominently placed, easily accessible across all connected devices and age appropriate by default.

5. Conclusions

Achieving effective industry self-regulation is never easy, especially in a rapidly changing, multi-jurisdictional, multi-stakeholder dominated online environment.

This article analyzed four specific self-regulatory initiatives aiming to protect online child privacy. A formal self-regulatory process analysis focused on the procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors) aspects of the initiatives, and demonstrated significant limitations of self-regulation in the area of online child safety compared to the area of online advertising. The former suffers from limitations due to broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often inexistent sanctions. The comparison provides an opportunity to distinguish several features that can possibly contribute to greater effectiveness of the self-regulatory schemes to protect the online privacy of children.

First, clearly defined voluntary rules and measurable standards, rather than a broad statement of objectives, can enable better adoption and action of the voluntary initiatives in practice. In addition, formal approval of the industry formulated rules by public authorities can help to take into account public interests. However, it has been recognized that refined and detailed rule-making is possible when the rules aim to mitigate a single privacy risk, such as personal data misuse. Online child safety initiatives, where different risks and various aspects of social privacy are at stake, require multi-stakeholder dominated platforms which manage to agree only on broad statements and principles. They can hardly be prescriptive and provide technical implementations, as they inherently focus on desired outcomes, leaving a large margin of maneuver for implementation to individual companies. As a result, their adoption and implementation is inevitably more complicated and less measurable.

Second, lack of independent monitoring schemes and the absence of enforcement mechanisms and dissuasive sanctions in cases of malpractice in the majority of the online child safety initiatives could be mitigated by the availability of organizational structures for self-regulatory tasks. An industry association of a particular sector, through "institutionalization" of self-regulation, would not only provide the necessary personnel and organizational structures to enforce self-regulatory rules and impose fines for non-compliance, but also due to the additional benefit provided to its members, such as lobbying, education and training, could exercise a threatening power in case of exclusion. However, such stable structures do not exist yet in cases where multi-sectoral action to mitigate online privacy and safety risks is necessary.

Therefore, it has been argued that it would be more beneficial to tackle online child privacy issues separately from safety initiatives and use sectorial industry associations for the self-regulatory task. This would not only bring online privacy protection mechanisms more in line with the human rights perspective, but also lead to clear and more enforceable rules given the possibility for public authorities to approve their content and the similarity of the industry players.

Such a human rights-based approach, instead of a safety-based approach, would consequently require the EU to take a stronger and better defined co-regulatory strategy. The new General Data Protection Regulation envisions a similar future and encourages associations to adopt approved and monitored codes of conduct for the purpose of specifying the application of data protection provisions when processing children's personal data.

The aim of the online child safety initiatives to empower the users through technological solutions to manage their social privacy, instead, could be partially realized by putting more pressure on the industry to implement the privacy by design and privacy by default principles, also present in the Regulation.

Although the existing self-regulatory initiatives in the area of online child safety may be criticized, the broader potential of private governance networks in this domain should not be denied. Self-regulation "has advantages over no regulation at all" as even if doubtful in effectiveness it can overcome market failures and prevent violations of economic and privacy interests of the users (De Haan *et al.*, 2013, p. 112). Apart from effective or ineffective regulatory outcomes, the process of self-regulation alone may create innovation, permit mutual learning, awareness raising, sharing of resources among industry and other stakeholders. Due to the fact that the industry takes up the regulatory responsibility, some industry players may propose new technical solutions to protect children from online privacy risks (e.g. age-verification mechanisms, privacy by default measures, parental controls). From a user perspective, any improvement of privacy features and policies in online services and mutual change can be considered a sign of success of a regulatory process. The question is whether the initiatives that aim to bring industry together into networks for sharing knowledge and experience without adequate rules, monitoring and enforcement procedures should be called 'self-regulation' or this term should only be allowed "when it was surrounded by heavy qualifications or caveats" (Carr, 2015).

Notes

[1] Due to the significant degree of involvement and input on the part of the European Commission into the online child safety self-regulatory initiatives, it is difficult to apply a clear categorization to the adopted initiatives and label them self-regulation or co-regulation. Given the existing rich typology of Internet co-regulation and the difficulty of clearly separating self-and co-regulation both as concepts and as practices, this paper refers to the initiatives under analysis as self-regulatory initiatives. It uses the term 'self-regulation' in a broad sense, encompassing a process of rule setting wherein the industry alone or together with other stakeholders formulates the rules, enforces and adjudicates them. In this sense, it follows the definition of self-regulation provided by the EU itself in point 22 of the Interinstitutional Agreement on Better Law Making (OJ EU 321/1, 31.12.2003), denoting "the possibility for economic operators, the social partners, non-governmental organizations or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements)".

[2] For the sake of comprehensiveness, one additional self-regulatory initiative should be mentioned - The European Framework for Safer Mobile Use by Young Teenagers and Children (2007) Available from URL: http://www.gsma.com/gsmaeurope/wp-content/uploads/2012/04/saferchildren.pdf [Last accessed 20 December 2014]. This initiative is excluded from the analysis in this paper because it focuses merely on online child safety, excluding online privacy from its content.

[3] The existence of similar international initiatives, such as the IAB Europe EU framework for Online Behavioural Advertising ([Last accessed 20 July 2015] Available from URL: http://www.iabeurope.eu/files/5013/8487/2916/2013-11-11_IAB_Europe_OBA_Framework.pdf) and the

EASA Best Practice Recommendation on Online Behavioural Advertising 2011 ([Last accessed 20 July 2015], Available from URL: http://www.easa-alliance.org/page.aspx/386) should be acknowledged. However, due to the lack of substantial provisions on children's privacy (they entail only a prohibition to create segments for online behavioural advertising purposes that are specifically designed to target children under the age of 12) and the overall focus of this paper on the European level, these self-regulatory initiatives were left outside the scope of the paper.

[4] ICT Coalition, 'A brief description who we are'. [Last accessed 1 May 016]. Available from URL: http://www.ictcoalition.eu

[5] The exact implementation of the FEDMA Code rules is left to the national direct marketing associations (DMAs) and may vary from country to country. Some DMAs can go further than the Code requirements and reformulate as well as implement the rules more rigidly, some can just take the principles and adapted them in their national codes while some other simply translate the FEDMA Code into their language.

[6] See for example, European Commission - Press release, 2011, Digital Agenda: only two social networking sites protect privacy of minors' profiles by default. [Last accessed 29 July 2014]. Available from URL: http://europa.eu/rapid/press-release_IP-11-762_en.htm

References

A29WP (Article 29 Data Protection Working Party) (2003) Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing, WP 77, 13 June 2003.

A29 WP (Article 29 Data Protection Working Party) (2010) Opinion 4/2010 on the European code of conduct of FEDMA for the use of personal data in direct marketing, WP 174, 13 July 2010.

Ayres I, Braithwaite J (1992) *Responsive Regulation: Transcending the Deregulation Debate.* Oxford University Press, Oxford.

Barlow J.P. (1996) A Declaration of the Independence of Cyberspace. [Last accessed 20 June 2015]. Available from URL: https://projects.eff.org/~barlow/Declaration-Final.html

Bennett C. J. (2004) Privacy Self-Regulation in a Global Economy: A Race to the Top, the Bottom or Somewhere Else? In: Webb K (ed), *Voluntary Codes: Private Governance, the Public Interest and Innovation,* pp. 227-249. Carleton University, Ottawa.

Bonnici M.J.P. (2008) *Self-regulation in Cyberspace*, T.M.C. Asser Press, The Hague.

Bowman D.M., Hodge G.A. (2009) *Counting on codes: An examination of transnational codes as a regulatory governance mechanism for nanotechnologies* **,**Regulation & Governance 3(2), pp. 145-164.

boyd d. (2014) *It's Complicated: The Social Lives of Networked Teens*, Yale University Press, New Haven, CT.

Carr J (2015) Big Brains in Berlin [Blog post]. [Last accessed 20 June 2015] Available from URL: https://johnc1912.wordpress.com/2015/04/22/big-brains-in-berlin/

Cave J, Marsden C, Simmons S (2008) Options for and Effectiveness of Internet Self- and Co-Regulation. RAND Europe. [Last accessed 20 June 2015] Available from

URL:http://ec.europa.eu/dg/information_society/evaluation/data/pdf/studies/2006_05/phase2.pdf

CEO Coalition (2011) Statement of Purpose. [Last accessed 29 July 2014]. Available from URL: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ceo_coalition_statement.pdf

CEO Coalition (2012) Report of Mid-term review meeting of the CEO Coalition to make the Internet a better place for kids (2012). [Last accessed 29 July 2014]. Available from URL: http://ec.europa.eu/information_society/activities/sip/docs/ceo_coalition/report_11_july.pdf

CEO Coalition (2013) Summary report. [Last accessed 20 June 2015] Available from URL: https://ec.europa.eu/digital-agenda/node/61973

CEO Coalition (2014) Progress reports on actions to make the Internet a Better Place for Kids. [Last accessed 20 June 2015] Available from URL:http://ec.europa.eu/newsroom/dae/itemdetail.cfm?item_id=14391

CoP (Community of Practise) (2013) Principles for Better Self- and Co-Regulation. [Last accessed 20 June 2015] Available from URL: http://ec.europa.eu/digitalagenda/sites/digitalagenda/files/CoP%20-%20Principles%20for%20better%20self-%20and%20co-regulation.pdf

De Haan J, Van der Hof S, Bekkers W, Pijpers R (2013) Self-regulation. In: O'Neill B, Staksrud E, McLaughlin S (eds.) *Towards a better Internet for Children. Policy pillars, player and paradoxes*, pp. 111-129. Nordicom, Gothenburg.

Doig A, Wilson J (1998) The Effectiveness of Codes of Conduct. *Business Ethics: A European Review* 7, 140-149.

Donoso V (2011) Results of the Assessment of the Implementation of the Safer Social Networking Principles for the EU. Individual Reports of Testing of 14 Social Networking Sites. European Commission, Safer Internet Programme, Luxembourg.

EDRi (European Digital Rights) (2013) *CEO Coalition - the blind leading the bland*. [Last accessed 20 June 2015] Available from URL:http://edri.org/ceo_coalition.

European Commission (1996) Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, COM (1996) 483 final.

European Commission (2006) Communication from the Commission - Towards an EU strategy on the rights of the child, COM(2006) 0367 Final.

European Commission (2009) Safer Social Networking Principles for the EU. [Last accessed 29 January 2015]. Available from URL:https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/sn_principles.pdf .

European Commission (2010) Summary of Replies to the Public Consultation about the Future Legal Framework for Protecting Personal Data, 4 November 2010. [Last accessed 29 July 2014]. Available from URL:http://ec.europa.eu/justice/news/consulting_public/0003/summary_replies_en.pdf .

European Commission (2012) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children, COM(2012) 196 Final.

European Commission (2015) Inception Impact Assessment, REFIT Evaluation and Impact Assessment of the EU Audiovisual Media Services Directive 2010/13/EU (AVMSD). [Last accessed 15 May 2016] Available from URL: http://ec.europa.eu/smart-regulation/roadmaps/docs/2015_cnect_006_cwp_review_avmsd_iia_en.pdf

FEDMA (2003) FEDMA European Code of Practice for the Use of Personal Data in Direct Marketing. [Last accessed 20 June 2015] Available from URL: http://www.fedma.org/fileadmin/documents/SelfReg_Codex/FEDMACodeEN.pdf

FEDMA (2010) European Code of Practice for the use of personal data in direct marketing electronic communications Annex. [Last accessed 20 December 2014]. Available from URL: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp174_annex_en.pdf

Gunningham N (1995) Environment, Self-regulation, and the Chemical Industry: Assessing Responsible Care. *Law & Policy* 17, 57-109.

Gunningham N, Grabosky P (1998) *Smart Regulation: Designing Environmental Policy.* Oxford University Press, Oxford.

Gunningham N, Rees J (1997) Industry Self-regulation: An Institutional Perspective. *Law & Policy* 19, 363-414.

ICT Coalition (ICT Coalition for Children Online) (2012) ICT Principles. [Last accessed 29 January 2015]. Available from URL:http://www.ictcoalition.eu/.

Jenkins R (2001) *Corporate Codes of Conduct: Self Regulation in a Global Economy.* United Nationals Research Institute for Social Development, Geneva.

Kohler-Koch B (2002) European Networks and Ideas: Changing National Policies? *European Integration Online Papers*, 6(6).

Kooiman J (2003) *Governing as Governance*. Sage, London.

Koops B.J, Prins C, Schellekens M, Lips M (eds) (2006) *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-liners*. Information Technology & Law Series (9). T.M.C. Asser Press, The Hague.

Latzer M, Just N, Saurwein F (2013) Self- and co-regulation: evidence, legitimacy and governance choice. In: Price M E, Verhulst S G, Morgan L (eds), *Routledge Handbook of Media Law*, pp. 373-397. Routledge, Abingdon / New York.

Latzer M, Price M.E., Saurwein F, Verhulst S.G. (2007) *Comparative Analysis of International Co- and Self-regulation in Communication Markets*, Research report. OFCOM, Vienna.

Lievens E (2010) *Protecting Children in the Digital Era: the Use of Alternative Regulatory Initiatives*. Martinus Nijhof Online, Leiden.

Livingstone S (2011) Regulating the Internet in the Interests of Children: Emerging European and International Approaches. In: Mansell R. Raboy M (eds) *The Handbook of Global Media and Communication Policy*, pp. 505-524. Wiley-Blackwell, Oxford.

Livingstone S, Haddon L, Görzig A, Ólafsson K (2011) *Risks and safety on the Internet: The perspective of European children.* Full Findings. LSE, EU Kids Online, London.

Livingstone S, Ólafsson K, O'Neill B, Donoso V, (2012) *Towards a better internet for children: findings and recommendations from EU Kids Online to inform the CEO coalition.* LSE, EU Kids Online, London.

Livingstone S, Ólafson K, Staksrud E (2013) Risky Social Networking Practises among "underage" Users: Lessons from Evidence-Based Policy.*Journal of computer-Mediated Communications*, 303-320.

March D (1998) *Comparing policy networks*, Open University Press, Buckingham.

Mascheroni G, Ólafsson K. (2014) Net children go mobile: risks and opportunities (2nd ed.). Educatt, Milan.

O'Neill B (2014) First report on the Implementation of the ICT Principles. The ICT Coalition for the Safer Use of Connected Devices and Online Services by Children and Young People in the EU, Brussels. [Last accessed 20 June 2015] Available from URL: http://www.ictcoalition.eu/

O'Neill B, Livingstone S, McLaughlin S (2011) Final recommendations for policy, methodology and research. LSE, EU Kids Online, London.

O'Neill B, Staksrud E, Mclaughlin S (2013) *Towards a better internet for children: policy pillars, players and paradoxes*. Nordicom, Gothenburg.

Rees J (1997) *The Development of Communitarian Regulation in the Chemical Industry. Law and Policy 19, 477-528.*

Rhodes R.A.W. (1997) *Understanding Governance. Policy Networks, Governance, Reflexivity and Accountability*. Open University Press, Buckingham.

Schulz W, Held T (2002) Regulierte Selbstregulierung als Form modernen Regierens. Im Auftrag des Bundesbeauftragten für Angelegenheiten der Kultur und der Medien, Arbeitspapiere des Hans-Bredow-Instituts nr. 10. Verlag Hans-Bredow-Institut, Hamburg.

Scott C, Cafaggi F, Senden L (2011) The Conceptual and Constitutional Challenge of Transnational Private Regulation. *Journal of Law and Society* 38(1), 1-19.

Scott C (2012) Beyond Taxonomies of Private Authority in Transnational Regulation. *German Law Journal* 13, 1329-1338.

Sethi S.P., Emelianova O (2006) A Failed Strategy of Using Voluntary Codes of Conduct by the Global Mining Industry. *Corporate Governance: The International Journal of Effective Board Performance* 6, 226-238.

Staksrud E, Lobe B (2010) Evaluation of the implementation of the Safer Social Networking Principles for the EU Part I: General Report. European Commission Safer Internet Programme, Luxembourg.

Van der Hof S (2014) No Child's Play: Online Data Protection for Children. In: Van der Hof S, Van den Berg B, Schermer B (eds) *Minding Minors Wandering the Web - Regulating Online Child Safety*, pp. 127-141. TMC Asser Press / Springer Press, The Hague.

Verbruggen P (2013) *Gorillas in the closet? Public and private actors in the enforcement of transnational private regulation,* Regulation & Governance 7(4), pp. 512-532

Verbruggen P (2014) *Enforcing Transnational Private Regulation: A Comparative Analysis of Advertising and Food Safety*. Edward Elgar, Cheltenham.

Webb K (2004) Understanding the Voluntary Codes Phenomenon. In: Webb K (ed), *Voluntary Codes: Private Governance, the Public Interest and Innovation,* pp. 3-35. Carleton University, Ottawa.

Webb K, Morrison A (2004) The Law and Voluntary Codes: Examining the "Tangled Web." In: Webb K (ed) *Voluntary Codes: Private Governance, the Public Interest, and Innovation*, pp. 97-174. Carleton University, Ottawa.

Weber R.H. (2002) *Regulatory models for the Online World*. Schulthess, Zurich.

Weber R.H. (2012) Future Design of Cyberspace Law-"Laws are Sand" (Mark Twain, The Gorky Incident), *Journal of Politics and Law* 5(4).

Westin A. F (1967) *Privacy and freedom*. 1st ed. Atheneum, New York.

Chapter 8

Conclusions

The overall ambition of this PhD dissertation was to contribute to a better understanding and justification of the necessity of specific regulatory privacy protection (through legal and soft-law tools) for children on the internet, to identify the exising gaps and unclarities, and consequently to consider how to improve existing regulation. In doing so, the research for this dissertation was guided by the following central research question: how can the EU law and self-regulatory initiatives protect children from online privacy risks while accounting for the particular characteristics of children. This concluding chapter summarises the arguments made in the previous chapters by outlining the main findings and grouping them according to the research sub-questions.

1. Beyond the obvious and explicit: a multitude of raisons d'être for a child-specific privacy protection regime

The first research sub-question, implied by the main research question, was: What are the characteristics that make the (online) position of children special and require a specific regime to protect them from privacy risks online in the EU?

This dissertation identified explicit and implicit types of justifications for specific protection going beyond data protection law and drawing attention to children not only as data subjects but also as consumers and as young, still developing, individuals. The analysis suggested that in addition to the lack of knowledge and implications of personal data collection practises (the GDPR lack of knowledge yardstick), children merit enhanced protection due to their different online behaviour, needs and privacy perceptions, their potential vulnerability as a result of their different psychological and cognitive characteristics, and their special privacy-related interests.

1.1. The lack of knowledge yardstick

The GDPR refers to the lower awareness as a yardstick to normatively justify establishing its specific child's data protection regime.

Lack of knowledge and the absence of a full understanding of complex personal data collection practices, along with their implications, especially online, is an undeniable problem not only for children and young people, but for many adults too. Empirical research shows that some more advanced data collection and tracking techniques and their possible impact, are hardly understandable even for sophisticated users. Websites that are popular among children employ increasingly sophisticated methods to gather children's data as they play, communicate or browse online, resulting in their constant surveillance. Privacy policies are long, complex, difficult to find and often age-inappropriate.[947] The privacy policies of the most widely used

[947] Micheti A Burkell J and Steeves V (2010) Fixing Broken Doors: Strategies for Drafting Privacy Policies Young People Can Understand. Bulletin of Science, Technology & Society 30(2): 130-143; Grimes S (2013) Persistent and emerging questions about the use of end-user licence agreements in children's online games and virtual worlds. UBC Law Review 46 (3): 681-791.

social networking sites, are framed in language which valorises 'sharing' and 'control', despite the ongoing ubiquitous collection, use and disclosure of their data.[948] Even though some children might be tech-savvy and informed internet users, a stance which has been widely debated in the academic literature[949], this does not necessarily render them capable of fully realising the consequences of pervasive online data collection practices.

1.2. Different online behaviour, needs, and privacy perceptions

The GDPR refers only to the (lack of) certain capacities pertaining to children rather than to the specific features characterizing children and, especially, teenagers as individuals. Development psychology provides evidence that adolescents have particular needs and interests, such as identity formation, developing their agency and establishing autonomy, creating peer relations.[950]

Relationship development is an important need during adolescence. Making friends and forming peer relations become increasingly important with growth and can even affect the psychological, social and academic development of the adolescents.[951] Adolescents are eager to make new friends[952] and often establish more friendships than adults.[953] These assumptions are confirmed in the social media context: younger social media users tend to create new relationships more often, while older users often strengthen ties with the existing friends.[954]

---

[948] Steeves V (2016) Terra Cognita: The Surveillance of Young Peoples' Favourite Websites. In Rooney T and Taylor E (eds) Surveillance and Childhood, United Kingdom: Ashgate Publishing Limited, 1-36. Montgomery K (2015) Youth and surveillance in the Facebook era: Policy interventions and social implications, Telecommunications Policy 39: 771-786.

[949] Helsper E J and Eynon R (2010) Digital natives: where is the evidence?, British Educational Research Journal 36(3): 503-520. Bennett S, Maton K and Kervin L (2008) The 'digital natives' debate: A critical review of the evidence. British Journal of Educational Technology, 39(5): 775-786. Chung G and Grimes S (2005) Data Mining the Kids: Surveillance and Market Research Strategies in Children's Online Games. Canadian Journal of Communication 30: 527-548. Valkenberg V and Cantor J (2002) The Development of a Child into a Consumer. In Calvert S, Cocking, R, and Jordan A (eds) Children in the Digital Age, New York: Praeger, 201-214.

[950] Greenfield P (2008) Living online: Implications for development and developmental methodology. *ISSBD Newsletter* 2(54):1–4; Greenfield P M, Gross E F, Subrahmanyam K, Suzuki L K, Tynes B (2006) Teens on the Internet: Interpersonal connection, identity, and information. In R. Kraut (ed), *Information technology at home*, New York: Oxford University Press; Subrahmanyam K (2008) Communicating online: Adolescent relationships and the media, The Future of Children. *Children and Media Technology* 18: 119–146; Subrahmanyam K, Eddie C M G, Harsono L S, Janice S L, & Lawrence L (2009). In their worlds: Connecting online weblogs to developmental processes. *British Journal of Developmental Psychology* 27: 219–245;

[951] Blieszner, R., & Roberto, K. A. (2004). Friendship across the life span: reciprocity in individual and relationship development. In F.R. Lang & K.L. Fingerman (eds.), Growing together: personal relationships across the lifespan, 159–182. Cambridge, UK: Cambridge University Press; Savin-Williams, R. C., & Berndt, T. J. (1990). Friendship and peer relations. In S.S. Feldman & G. Elliot (eds.), At the threshold: The developing adolescent, 277-307. Cambridge, MA: Harvard University Press.

[952] Boneva, B.S., Quinn, A., Kraut, R.E., Kiesler, S., & Shklovski, I. (2006). Teenage communication in the instant messaging era. In R. Kraut, M. Brynin, & S. Kiesler (eds.) Computers, phones, and the Internet: Domesticating information technology, 201-218. Oxford, New York: Oxford University Press.

[953] Hartup, W.W. & Stevens, N. (1999). Friendships and adaptation across the life span. Current Directions in Psychological Science, 8(3), 76-79; Blieszner, R., & Roberto, K. A. (2004). Friendship across the life span: reciprocity in individual and relationship development. In F.R. Lang & K.L. Fingerman (eds.), Growing together: personal relationships across the lifespan, 159–182. Cambridge, UK: Cambridge University Press.

[954] Wouter Steijn, Developing a sense of privacy, Phd dissertation, 2014, https://pure.uvt.nl/ws/files/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf, Steijn and

During adolescence identity creation and self-representation in from of friends is a key need.[955] Social media has become a new arena for adolescents to present and experiment with their identities.[956] Identity development and creation of relations as developmental needs are potentially connected with user online behaviour, such as adding contacts on their social networks and disclosure of personal information.[957]

Academics have established the link between developmental phases and online behaviour in relation to adolescents.[958] Empirical research also hase elucidated that privacy perceptions and concerns are different between children, adolescents and adults and the developmental perspective can help to understand, and thus justify, the different privacy concerns and behaviour between individuals of different age on social media.[959]

Yet, the key features of social networks that strongly meet adolescent needs and manipulative and unfair techniques to satisfy those needs often used online[960] have raised concerns among academics and policy makers. As a result, questions have emerged as to whether certain data collection and use practices directed to children, such as intrusive and negative-impact having profiling or emotional manipulation, should be considered unfair commercial practices in terms of consumer law and should be added to a blacklist of the Unfair Commercial Practices Directive.

1.3. Particular vulnerabilities and immaturities

The reliance on neurotechnology, in particular magnetic resonance imaging, in the last decade has provided neurological evidence to compare the different structures and functioning of adolescent and adult brains. Scientists have demonstrated that there are structural and functional immaturities in the brain of adolescents. Since the part of the brain controlling inhibitions fully matures only in early adulthood, adolescents can be less capable of evaluating risky situations and can be more easily misled.[961] They are less likely to consider the long-

Schouten 2013. Mantelero A (2016) Children online and the future EU data protection framework: empirical evidences and legal analysis. *International Journal of Technology Policy and Law* 2(2–4): 169–181

[954] Amanda Third et al., 'Children's Rights in the Digital Age: A Download from Children Around the World' (Young and Well Cooperative Research Centre, Melbourne, 2014).

[955] Erikson, E.H. (1959). Identity and the life cycle. New York: Norton

[956] Valkenburg, P.M., & Peter, J. (2008). Adolescents' identity experiments on the internet: consequences for social competence and self-concept unity. Communication Research, 35(8), 208-231.

[957] boyd, d.m. (2008). Taken out of context: American teen sociality in networked publics. PhD thesis, University of California, Berkeley. Boneva, B.S., Quinn, A., Kraut, R.E., Kiesler, S., & Shklovski, I. (2006). Teenage communication in the instant messaging era. In R. Kraut, M. Brynin, & S. Kiesler (eds.) Computers, phones, and the Internet: Domesticating information technology, 201-218. Oxford, New York: Oxford University Press; Marwick, A.E., Diaz, D.M., & Palfrey, J. (2010). Youth, privacy and reputation. Literature review. Berkman Center Research Publication No. 2010-2015; Harvard Public Law Working Paper No. 2010-2029; Peter, J., & Valkenburg, P. (2011). Adolescents' online privacy: toward a developmental perspective. In S. Trepte & L. Reinecke (eds.), Privacy online, 221-234. Heidelberg: Springer

[958] Peter, J., & Valkenburg, P. (2011). Adolescents' online privacy: toward a developmental perspective. In S. Trepte & L. Reinecke (eds.), Privacy online, 221-234. Heidelberg: Springer

[959] Wouter Steijn, Developing a sense of privacy, Phd dissertation, 2014, https://pure.uvt.nl/ws/files/7737309/Steijn_Developing_05_09_2014_emb_tot_06_09_2015.pdf

[960] Montgomery K (2015) Youth and surveillance in the Facebook era: Policy interventions and social implications, Telecommunications Policy 39: 771-786.

[961] Giedd J N (2008) The Teen Brain: Insights from neuroimaging, Journal of Adolescent Health, 42(4):335–343. McAnarney E R (2008) Adolescent Brain Development: Forging New Links?. Journal of Adolescent Health, 42(4): 321–323. McCreanor, T Barnes H M, Gregory M, et al. Consuming identities: Alcohol marketing and the commodification of youth experience. Addiction Research & Theory, 13 (6): 579–590.

term consequences of their actions, and are more likely to be risk-prone.[962] As summarised by Preston and Crowther, "(N)otwithstanding growing research on the capabilities of teenagers and their need for respect and autonomy, the developmental science shows that, alongside these positive qualities, minors are nonetheless still impulsive, take more risks than adults, and are less capable of controlling their emotions"[963]. They continue: "(t)hese behavioral immaturities suggest that minors are not in the same position as adults when making long-term decisions, especially when surrounded by their peers" and note further that "in the Internet age, they are always surrounded by their peers, using social media to bounce every decision off a host of other teenagers"[964]. This has resulted in the questioning of Jean Piaget's previously dominant claim that by the age of 15, adolescents' cognitive capability to understand, appreciate, and articulate decisions are on par with those of an adult.[965] It has been instead acknowledged that "teenagers may have the *ability* to reason like adults, but do so with vexing inconsistency"[966] due to, among others, their emotional volatility, impulsiveness, lower ability to deflect the pressure of peers.

It should be pointed out that the research results on adolescents' brain have not been free of criticism. Bessant, for example, criticised this research as "it begins with a prejudice ('they' are 'different' 'irrational' and 'deficient') and then threatens to expand the civil and social disadvantages that already severely affect too many of our young people". [967] By contrast, she claimed that "some young people are sometimes at risk not because their brains are different, but because they have not had the experience or opportunity to develop the skills and judgment that engagement in those activities and experiences supply".[968]

Nevertheless, the specific developmental features might influence adolescents' online behaviour and increase the possibility of online victimisation among peers, as well as the possibility of commercial personal data exploitation to a level higher than that of cases involving younger children or adults. In the commercial context, such exploitation can be seen when online marketers employ special strategies to take advantage of the adolescent's vulnerabilities, knowing that '(b)ecause of adolescents' emotional volatility and their tendency to act impulsively, they are also more vulnerable than adults to such techniques as real-time bidding, geolocation targeting (especially when an individual is near a point of purchase), and 'dynamic creative' ads tailored to their individual profiles and behavior patterns'.[969] Data protection and its justification could be significantly strengthened or even refined if the law were informed by or even incorporate some of the main finding on minors from developmental psychology and neurosciences. As claimed by Preston and Crowther, "(w)hen approached carefully and consistently, scientific research can be successfully integrated into our legal structure, infusing it with greater understanding and ability to meet the needs and realities of

Steinberg L (2007) Risk taking in adolescence: New perspectives from brain and behavioral science. Current Directions in Psychological Science 16 (2): 55–59. Steinberg L (2008) A social neuroscience perspective on adolescent risk-taking. Developmental Review 28 (1): 78–106.

[962] Ibid.

[963] Preston, Cheryl B. and Crowther, Brandon T. (2014) " Legal Osmosis: The Role of Brain Science in Protecting Adolescents," Hofstra Law Review 43(2), 454.

[964] Ibid.

[965] Cited in Preston, Cheryl B. and Crowther, Brandon T. (2014) " Legal Osmosis: The Role of Brain Science in Protecting Adolescents," Hofstra Law Review 43(2), 454-455.

[966] Ibid.

[967] Judith Bessant, 'Hard wired for risk: neurological science, 'the adolescent brain' and developmental theory', (2008) 11(3) Journal of Youth Studies 347, 358.

[968] Ibid.

[969] Montgomery K (2015) Youth and surveillance in the Facebook era: Policy interventions and social implications, Telecommunications Policy 39: 771-786, 777.

adolescents rather than the panic of older generations or the self-interested demands of corporate and governmental pressure"[970].

EU consumer law, in contrast to the data protection law, has clearly distinguished a special category of 'vulnerable consumers' and provided justification for their protection.[971] Such justification is partially based on the insights from social sciences. Vulnerability in consumer law can be both "a permanent or long-term condition, often related to factors internal to the consumer, such as age, inexperience or a disability" and "dynamic and relative" in its nature arising in interaction with markets and services. Thus, any consumer can become vulnerable at times depending on his personal situation and characteristics as well as products or services and marketing used.[972] According to the recent interpretation of the vulnerability concept in the EU "(V)ulnerability is not a static condition. Consumers may move in and out of states of vulnerability and they may be vulnerable in respect of some categories of transaction but not others. In addition, vulnerability is best viewed as a spectrum rather than a binary state"[973].

Children and teenagers may be more vulnerable as consumers not only because they lack knowledge and skills, but also because (partially due of this lack) they can be more easily influenced by others (susceptibility).[974] Research on consumer socialisation deals with the development of consumer skills, knowledge and attitudes of children and adolescents.[975] It indicates that the ability to act as consumers is increasingly acquired with growth. Research on the ability to understand advertising demonstrates that younger children are not able to critically assess and understand persuasive aim of advertising.[976] From 7-8 years old children start to distinguish the persuasive intent and realise that advertisements can be deceptive or bias.[977] From 11 years old children become more sceptical in relation to advertisement and their intent and tactics.[978] However, these age thresholds of recognising and understanding advertisements are not absolute or certain. Oath et al. claim that not all children being 10 years old can understand the persuasive aim of advertisers.[979] Livingstone and Helsper show a more complex picture on the relationship between influence and age: "different processes of persuasion operate at different ages, precisely because literacy levels vary by age".[980] Also, the

[970] Preston, Cheryl B. and Crowther, Brandon T. (2014) " Legal Osmosis: The Role of Brain Science in Protecting Adolescents," Hofstra Law Review 43(2), 454.

[971] It should be acknowledged that regulation of unfair commercial practices concerns the economic behaviour of consumers. Data protection regulation does not explicitly encompass economic behaviour, but as mentioned above the distinction between paid and free services has become obsolete.

[972] Waddington L (2014) Reflections on the Protection of 'Vulnerable' Consumers under EU Law, Maastricht Faculty of Law Working Paper No. 2013-2.

[973] European Commission, Consumer vulnerability across key markets in the European Union, Final report, January 2016, xvii.

[974] Duivenvoorde B (2013) The protection of vulnerable consumers under the Unfair Commercial Practices Directive. *Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht, 2* (2), 69-79.

[975] Roedder J D (2008), Stages of Consumer Socialization: The Development of Consumer Knowledge, Skills, and Values from Childhood to Adolescence," in Curt Haugvedt, Paul Herr, and Frank Kardes (eds.), The Handbook of Consumer Psychology, LEA.

[976] Martin M.C, 'Children's understanding of the intent of advertising: A meta-analysis' (1997) 16 (2) Journal of Public Policy and Marketing 205–216; Rozendaal E. et al., 'Reconsidering advertising literacy as a defense against advertising effects' (2011) Media Psychology 338–344.

[977] Roedder J D (2008), Stages of Consumer Socialization: The Development of Consumer Knowledge, Skills, and Values from Childhood to Adolescence," in Curt Haugvedt, Paul Herr, and Frank Kardes (eds.), The Handbook of Consumer Psychology, LEA.

[978] Ibid

[979] Oates, C., Blades, M., Gunter, B.& Don, J. (2003). Children's understanding of television advertising: a qualitative approach. Journal of Marketing Communications, 9, 59-71, 69.

[980] Blades, M., C. Oates, F. Blumberg, B. Gunter (eds), Advertising to Children: New Directions, New Media, 2016

findings on age ranges often reflect the research outcomes in the context of traditional advertising, such as on television or in newspapers, but are not to be directly transferred into the online context. Recognition of sophisticated advertising techniques in new media among children is much less explored than in traditional media. Yet, a recent EU study showed that although the most popular online games provide embedded or contextual advertisements, children have difficulty in recognizing marketing intend of the content, in shielding themselves from it and in taking decisions.[981] The impact of imbedded advertising is considerable on children from subliminally changing their behaviour and purchasing.[982]

It therefore could be claimed that children can be considered more vulnerable than many other types of consumers. While many other groups of consumers would change the states of vulnerability by acquiring and losing external vulnerability factors, children would often fall under both groups of internal and external vulnerability factors. They would be permanently vulnerable depending on their personal situation and most of the times depending on characteristics of products, services and marketing techniques.

1.4. Specific privacy-related interests

Besides the general privacy-related interests (personal autonomy, dignity, intimacy and self-determination), there are some privacy-specific interests of children that data protection law can promote. It can allow for harmonious development and growth, and facilitate the unconstrained creation of a child's - still-developing - personality. Academic literature elucidates that privacy afforded to adolescents can enforce their developing attitudes and identities and be instrumental for their dynamic self-determination and participation.[983]

What has been explicitly underlined in case law relating to children's privacy by several national courts is the importance of privacy for persons who have not yet reached physical, psychological and intellectual maturity. In Germany, the Constitutional court explicitly recognised that children are 'persons-in-the-making' and they have a 'right to become [i.e., to freely develop into] a [full] person'. As a consequence, children deserve extra protection in so far as the collection and disclosure of their personal data must be more rigorously justified than for adults whose personality is already-developed. Similarly, the Supreme Court of Canada also underlined the 'undoubted constitutional significance' of children's privacy and the special necessity to protect it. In its case law, the Court has recognised the 'inherent vulnerability of children' and their 'diminished moral culpability'. It has held that the privacy of children should be equally, if not more strongly protected, than that of adults, not only to avoid concrete harms, such as labelling and stigmatization, but, fundamentally, to guarantee the physical and moral autonomy and the well-being of the individual.

The French data protection authority (CNIL) has equally described a child as lacking psychological, intellectual and physical maturity and as going through the process of constructing their personality 'through a series of metamorphoses'[984]. Due to their personality being in development, law considers children to be in need of special protection against themselves (negative decisions that they themselves may take) and third parties.

---

[981] European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behavior, March 2016, at: http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/final_report_impact_marketing_children_final_version_approved_en.pdf

[982] Ibid.

[983] Roger J. R. Levesque. Adolescence, Privacy, and the Law: A Developmental Science Perspective 2016.

[984] CNIL, Internet et la collecte de données personnelles auprès des mineurs. (2001) Report. Available at: http://www.ac-grenoble.fr/juniors/droits/mineurs.pdf

It should be acknowledged that the courts and the CNIL mentioned-above have to a large extent followed the 'deficit theory of the child', perceiving children as inherently vulnerable and in need of protection. This view has been the subject of academic debate.[985] Scholars following the new sociological perspective of childhood (discussed in the introduction of this dissertation), have, in contrast, viewed children as beings rather than beings in the making, and refused biological reductionism and age-based determinism. However, the latter perspective although largely absent in court decision has been acknowledged by the Article 29 Working Party incorporated both views expressing them through the static and the dynamic perspective.[986] From the static point of view, it views the child as a person "who has not yet achieved physical and psychological maturity" and from the dynamic point of view as a person "in the process of developing physically and mentally to become an adult"[987]. The Working Party clearly recognised that the rights of the child to privacy and data protection, including their exercise, should be ensured in such a way that both of these perspectives are respected.

2. The EU child-tailored privacy protection regime

Building on the analysis justifying the need for a specific regime to protect children from privacy risks online, the research turned to examine the following two research sub-questions:

- How has the child-specific online privacy protection regime thusfar been constructed, i.e. what are the different levels, rules and tools employed in the EU?
- What are the dilemmas and unresolved challenges in terms of particular characteristics and rights of children when implementing child-specific online privacy protection mechanisms in practice?

The dissertation portrayed protection of children's privacy in the EU as a multifaceted regime composed of the GDPR (age generic and age specific provisions), self-regulatory initiatives and enforced self-regulatory tools (DPIAs).

2.1. The GDPR

The newly adopted GDPR emphasises the need to better safeguard children online and expressly addresses conditions and requirements for lawful processing of children's personal data in relation to online services offered directly to them. To achieve this, the GDPR constructs a child-specific privacy protection regime consisting a two-tier system of protections.

2.1.1. The first tier – age generic GDPR provisions

The first tier of the regime is composed of general, age-generic GDPR provisions. Although these provisions apply equally to both adults and children, they have been framed by the EU legislator as specifically relevant to children and their online activities.

---

[985] Allison James and Alan Prout (eds.) Constructing and Reconstructing Childhood: Contemporary Issues in the Sociological Study of Childhood. London: Falmer, 1997.

[986] Article 29 Working Party (A29WP), 'Opinion 2/2009 on the protection of children's personal data (general guidelines and the special case of schools) WP 160', 11 February 2009.

[987] Ibid.

First, the most prominent provision is the right to erasure (right be forgotten), allowing children to remove content that may be damaging to their reputation and personality. Essentially, this right is not a novelty, but an updated and clarified version of the right of access, already present in Article 12 of the Directive 95/46/EC. As Recital 65 explains, this right is particularly relevant in cases where children's data is collected online based on their consent, when they are not fully aware of the risks arising from the processing of this data, and later want to remove such personal data. The right to erasure can be exercised notwithstanding the fact that an individual is no longer a child. Although the right to erasure (right to be forgotten) is particularly relevant with respect to children's data, the application of this right to children may be more problematic and complex than it is for adults. When deciding whether to delete children's data, a dynamic perspective should be taken into account. With time, a child may become a public figure, and his data may therefore change status from private (worth deleting) to public interest-related (worth preserving) data.[988]

The second age-generic but child-relevant GDPR provision refers to the right to data portability, potentially allowing internet users to shift from one service provider to another by moving their personal data. In fact, an easier exit from 'walled gardens', such as Facebook, can reinforce the ongoing trend of social media platform diversification[989] among children, and consequently empower children to choose more privacy-friendly online services.

Third, the provisions on data protection by design and by default, contribute to the empowerment of adults, but in particular children and hence their protection through technology in the online setting. These principles require data protection safeguards to be built into products and services from the initial stage of their development. Privacy-friendly default settings are expected to be the norm on social networks and mobile apps.[990]

Fourth, the Regulation also aims to protect data subjects though awareness raising and the provision of transparent information. It obliges data controllers to give information to all data subjects in a clear, audience-appropriate language at the time that their personal data is collected. Recital 58 frames this requirement in relation to children as giving information 'in such a clear and plain language that the child can easily understand'. The challenge that will be faced by data controllers in practice, however, is how to implement the transparency requirement in a meaningful way in the case of children.[991] Drawing on consumer protection law and practices, Chapter 4 propose several ways to reach child-tailored transparency (personalised information, participatory transparency and information in symbols).

Fifth, the GDPR relies on the data protection impact assessments for data controllers to evaluate risks when data processing is likely to result in a high risk to the rights and freedoms of natural persons. In the DPIA data controllers need to evaluate, "the origin, nature, particularity and severity of that risk" and mitigate the risk by appropriate measures or consult the supervisory authority prior to the processing (Recital 84 of the GDPR).

[988] Blume P (2015) The Data Subject. European Data Protection Law Review 1(4): 258 – 264.

[989] Cortesi S (2013) Youth Online: Diversifying Social Media Platforms and Practices. In: Gasser U, Faris R and Heacock R (eds) *Internet Monitor 2013: Reflections on the Digital World. Berkman Center Research Publication* (27): 16-17.

[990] European Commission (note 11).

[991] Savirimuthu J (2016) Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests? In: Iusmen I and Stalford H (eds) *The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions*. Opladen: Barbara Budrich Publishers, 221-257.

Although neither the GDPR in Article 35(3)[992] nor the Article 29 Working Party in its recent guidelines[993] explicitly ask for a mandatory DPIA for all the systems involving personal data about children, it acknowledges that the processing of vulnerable data subjects' data could require a DPIA. Also, given the fact that the GDPR establishes a non-exhaustive list of "high risk" data processing operations that are subject to the DPIA requirement, national data protection authorities might include children's data into their lists of data processing operations under the DPIA obligation (Article 35.4). Thus, as in many cases, the DPIA will need to be conducted when personal data about children is collected, especially before the creation and deployment of a new product or service. Chapter 6 proposed a way to approach the specific DPIAs for children and outlined the main component and their attributes that data controllers providing information society services to children should consider.

Last, the GDPR encourages associations to adopt approved and monitored codes of conduct for the purpose of specifying the application of data protection provisions when processing children's personal data. However, codes of conduct should achieve clear formulation, adoption and enforcement of voluntary rules. Chapter 7 analysed four existing self-regulatory and reflected on the strengths and shortcomings of the self-regulatory process in the area of online child privacy.

2.1.2. The second tier – child specific GDPR provisions

Along with the first, general tier GDPR provisions, the Regulation introduces two provisions specifically for children as data subjects. They impose obligations on external parties, i.e. negative obligations for data controllers to abstain from certain data collection practises, and positive obligations for parents to engage in activities to secure the effective enjoyment of their child's fundamental rights.

First, the GDPR prohibits certain potentially harmful data collection practices through restrictions on the profiling and marketing activities of data controllers. Recital 38 generally emphasises that specific protection should be afforded to children against marketing or profiling. Under Article 4(4), 'profiling' means any automated data processing activity that involves (a) automated processing of personal data; and (b) using that personal data to evaluate certain personal aspects relating to a natural person. Specific examples include analyzing or predicting aspects concerning a person's economic situation, personal preferences, interests, behaviour, and location. Recital 71 refers to automated decision making based on profiling and states that such a measure should not concern children. This seems to lead to the conclusion that the profiling of children should not be carried out and that automated decisions based on profiling that produce legal effects or similarly significantly affect the child are prohibited.

Given that the articles of the GDPR do not explicitly exclude children from profiling and the recitals are not legally binding, debates are still taking place about the extent to which automated decisions based on profiling of children are allowed. Many unclear questions remain. If profiling measures in relation to children are allowed by the GDPR, how strictly should Article 22 of the GDPR be interpreted? When do decisions have a significant effect on children and what is the effect? Should this effect be negative? Should measures involving automated decisions based on profiling that aim to benefit children and enhance their rights,

[992] The initial GDPR proposal published by the European Commission on 25 January 2012 included children's data among the data categories for which the DPIA was required. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final, 25 January 2012.

[993] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248, 4 April 2017.

i.e. have positive effect, be allowed and under what legal ground for the related data processing? Would children be asked for an explicit consent to be profiled, can such consent be informed and if yes, at what age? What additional safeguards are necessary to prevent major problems associated with (commercial) profiling, such as the lack of control over the profile, its possible use and abuse, or opaque steering of consumer choices?

Second, the Regulation requires a prior parental consent or authorisation before the processing of the personal data of children when they are directly offered 'information society services' (Article 8). It is the most controversial and complicated GDPR provision in relation to children. As a general rule, protection through the parental consent mechanism is applicable to children under the age of 16. However, 16 is not an absolute threshold, as Member States are allowed to apply a lower age limit, which nevertheless cannot be lower than 13 years. The parental consent requirements is applicable online, excluding offline data processing practises, such as those in the context of school or leisure activities.

The analysis of the legislative history of Article 8 in the GDPR provided in Chapter 3 revealed the lack of well-reasoned justifications and evidence in terms of the substantive requirements adopted in the final GDPR version. With most of the GDPR debate being focused around articles with a direct economic impact on data controllers' activities and the Digital Single Market rather than the protection of vulnerable data subjects, Article 8 witnessed only sporadic renewals of interest during the debates in the EU institutions.

The European Commission almost literally copied the parental consent requirement from COPPA in its proposal for the GDPR, without taking into account the criticisms related to ineffective parental consent and age verification mechanisms or considering any alternatives of a more nuanced approach to child protection. COPPA has been heavily criticised due to its limited scope (i.e. its applicability only to children below the age of 13), the ineffectiveness and burden of parental consent mechanisms for service operators, the possible impact on online anonymity, and the balance between parental and service provider responsibility.

Despite many valuable amendments being registered, the discussions at the European Parliament did not lead to major substantive changes in Article 8 of the GDPR either. The Council has only substantially deviated from the original GDPR proposal on the age of consent. It initially increased the age limit of consent to 16 years and in the last minute of negotiations took a flexible approach leaving the decision partially to the Member states. As a consequence, this left the EU without coherent and uniform age threshold in the European Digital Market and undermined the much-anticipated harmonisation effect of the GDPR. In summary, the EU institutions failed to employ an up-to-date means of assessment, question the age limit for consent, assess the impact on children's rights and the effectiveness of a particular formulation of the parental consent requirement, and to consider adopting a more nuanced version of parental consent.

2.2. Dilemmas and tension with child rights in the GDPR

Chapter 2 examined two dilemmas that the introduction of the child-specific rules into the GDPR has created: the 'empowerment vs protection' and the 'individualized vs average child' dilemma.

The GDPR in relation to children essentially entails empowering provisions (the right to erasure, the right to data portability, data protection by design and by default, transparency and awareness) and protective provisions (the prohibition of profiling, parental consent). Ideally, data protection law should protect children from privacy risks, such as commercial data exploitation and misuse, reputational damage and harm to one's identity, dignity and personal integrity, while also enhancing online opportunities and accounting for the growing

maturity of children. This requires a policy framework that not only imposes legal compliance requirements on data controllers, but that also adequately balances online risks and opportunities, e.g. empowers children while also addressing the needs of those who require greater protection.

The consent requirement formulated in Article 8 of the GDPR seems to place children under the strict over-protection of their parents and to distort the balance between empowerment and protection towards the latter. The consent requirement is fully applicable in all cases except for the preventive or counselling services offered directly to a child and the GDPR does not foresee consent exceptions for less risky data collection practices; the consent rule is very broad in scope and applies to all types of online services in different sectors; it does not formally require the involvement of children or give due weight to children's opinions. The GDPR makes no effort to adopt a sliding scale approach and increasingly recognise child's agency, foster children's participation in their own protection, as well as support coping and resilience through learning by doing. The adoption of broad parental oversight through the consent mechanism also raises questions as to whether and to what extent children will be able to enjoy the empowering rights, such as the right to erasure and data portability, without parental involvement.

Although there is a clear lack of rules on children's ability to exercise their data subject rights[994], it seems to be recognised that the age for consent and the age at which a child might exercise his data subject's rights (e.g. to access or rectify personal data) should not necessarily coincide. Children as data subjects should be able to exercise their rights as soon as they can demonstrate the capacity to do so. This view is supported by several data protection authorities.[995] The ICO in the UK provides the following criteria to be used when considering borderline cases: the level of maturity of the child, the nature of the personal data, any court orders on parental responsibility, duty of confidence, any consequences or detrimental effect to the child and any views of the child.[996] However, the Article 29 Working Party has stated that the right of access should normally be exercised by the child's legal representative in the interest of the child with children who are mature enough permitted to act jointly with their representatives and only in limited cases alone, such as in relation to the health data.[997]

There is seemingly more flexible approach to the exercise of data subject rights in contrast with the strict requirements in the case of consent in practice. For example, the data protection authority in Italy has suggested the age threshold for consent according to the GDPR

---

[994] See Annex 1, which demonstrates that no clear provisions or guidance exist in the EU Member States regulating children's as data subjects rights.

[995] ICO states: "*Even if a child is very young, data about them is still their personal data and does not belong to anyone else. It is the child who has a right of access to the information held about them. Before responding to a request for information held about a child, organisations should consider whether the child is mature enough to understand their rights. If the organisation is confident that the child can understand their rights, then it will respond to the child rather than the parent. What matters is that the child is able to understand (in broad terms) what it means to make a subject access request and how to interpret the information they receive as a result of doing so*." (see ICO, Information for the public, at: https://ico.org.uk/for-the-public/personal-information/). The Irish Data Protection Commissioner states: "*Legal guardians can make an access request on behalf of a child. However, once a child is capable of understanding their rights to privacy and data protection, the child should normally decide for themselves whether to request access to data and make the request in their own name.Where an organisation receives an access request from a legal guardian on behalf of a child who has had direct interaction with that organisation, and/or where that child is capable of understanding their own rights to privacy and data protection, the organisation must take account of the child's rights in deciding how to respond to the access request.*" (see Access Rights and Responsibilities: A guide for Individuals and Organisations, at: https://www.dataprotection.ie/documents/AccessGuidance.pdf)

[996] ICO, Subject access code of practice: Dealing with requests from individuals for personal information, 9 June 2017, at: https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf

[997] Article 29 Working Party (A29WP), 'Opinion 2/2009 on the protection of children's personal data (general guidelines and the special case of schools) WP 160', 11 February 2009

at 16 years.[998] The new Anti-cyberbullying Law[999], which allows the lodging of a complaint for the removal, blocking or takedown of personal data for underage victims of cyberbullying, sets instead the age limit of 14. A huge amount of confusion, however, surrounding a uniform interpretation of the positioning of age in relation to data subjects rights and its relationship with consent remains. The UK Government has recently expressed a view that children should be able to ask for posts to be deleted at the age of 18.[1000] The logic appears to target the removal of past posts when a child reaches 18. There is no good reason, however, why a child should not be able to ask for blog posts to be removed at 16 or 17, or even younger. Children aged 16 or 17 are very likely to have the capacity to understand the issue and the process of asking for the deletion of information posted by others. The prohibition to exercise the data subjects rights until one reaches the legal majority would seem illogical and would undermine the very essence of the right to data protection. In theory, there also seems to be a recognition that an indication of the degree of maturity and autonomy, and thus the ability to exercise the rights of the data subject, is an analysis of the factual circumstances and thus whether the data concerned were provided by the parents or by the child. In other words, the exercise of data subject rights relies on the capacity to consent.

Nevertheless, it is important to keep in mind that there is a difference between accessing one's data (ex post control), and taking an active decision to authorize certain usage or disclosure of personal data that may have long-term consequences (ex ante control). John Eekelaar emphasises that "information sharing is a more complex issue than subject access",[1001] while Joan Loughrey has opined that:

> *'(c)hoosing to have your confidentiality breached is much more of an autonomy right. You need to have the capacity to make an autonomous decision regarding the release of information.'*[1002]

In sum, the highly protective consent provision seems to distort the balance between empowerment and protection towards the latter, especially for teens, and there is a risk that the same protective stance can be followed when interpreting the age threshold for data subjects' rights.

Although the maturity of the child (physical, emotional, cognitive and social development) should guide the balancing of the protection and empowerment elements, it is difficult to assess when an individual child is competent to take responsibility for a decision affecting him or her. This is the second 'individualized versus average child' dilemma discussed in this dissertation. This dilemma refers to the difficulty of determining the age at which specific protection for children should be lowered, taking into account the individual understanding and maturity of each child. Strict age thresholds or bright-line rules are absolute

---

[998] Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali, 28 April 2017, at: http://www.garanteprivacy.it/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali

[999] Legge 29 maggio 2017, n. 71

[1000] The Queen's Speech and Associated Background Briefing, On the Occasion of the Opening of Parliament on Wednesday 21 June 2017. The Speech refer to the aim 'to give people new rights to "require major social media platforms to delete information held about them at the age of 18"', p. 46, at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/620838/Queens_speech_2017_background_notes.pdf

[1001] Cited in Dowty, T. / Korff, D. (2009), Protecting the virtual child – the law and children's consent to sharing personal data, Study prepared for ARCH - Action on Rights for Children- and the Nuffield Foundation, 16, available at: http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf

[1002] Cited in Dowty, T. / Korff, D. (2009), Protecting the virtual child – the law and children's consent to sharing personal data, Study prepared for ARCH - Action on Rights for Children- and the Nuffield Foundation, 16, available at: http://www.nuffieldfoundation.org/sites/default/files/Protecting%20the%20virtual%20child.pdf

blanket norms, they do not allow for the examining of the best interests of each child on a case-by-case basis, or for the taking into account of individual ability and development. They are based on a generalized age limit that is used as a proxy for maturity and judgement, and thus may easily exclude children capable of maturely engaging in certain activities. Yet, the capacities of a child are personal, context-dependent and constantly evolving. An assessment in each individual case would show widely differing capacities among children of the same age and could, thereby, reflect the best interests of the child. In addition, the same child may need protection for one data processing purpose, and autonomy or self-determination for another, depending on the potential privacy risks and harm that are at stake. The imposition of legal age limits may disproportionally restrict the rights of other children and data subjects, irrespective of a child's own levels of competence.

2.3. Lack of legal certainty and effectiveness

Chapter 3 showed that the GDPR parental consent requirement lacks legal certainty and faces many practical challenges related to its implementation. First, the parental consent requirement is applicable to information society services offered directly to a child. As information society services are normally provided for remuneration, this causes uncertainty as to the particular material scope of Article 8, especially its applicability to free services. Second, the requirement concerns online services offered directly to children, but it is complicated to draw the exact distinction between services to which the protection should apply. The extent to which the GDPR parental consent requirement will cover general-audience or mixed-audience services and sites remains unclear. The FTC solution of subjecting different services to a parental consent requirement through the 'totality of the circumstances test' and 'actual knowledge test' is useful, despite its flaws. Third, as the GDPR allows consent authorisation by the parents or the holders of parental responsibility over the child, it remains unclear if the reference to consent authorisation can be understood as allowing a joint consent and if the circle of holders of parental responsibility can include individuals other than parents and legal guardians. Fourth, to comply with the GDPR it suffices to make reasonable efforts to obtain verifiable parental consent rather than guarantee verified consent as a final outcome. It is not clear how much effort and proof in relation to obtaining consent can be requested from the controllers in order to sufficiently demonstrate compliance nor how reasonable efforts should be documented and proven. Fifth, specific parental consent mechanisms that can be used by data controllers to be compliant with the GDPR require further clarification and the guidance of the FTC on COPPA can be informative in specifying adequate and GDPR-compliant consent verification methods. Finally, the GDPR does not explicitly require the verification of a child's age, and thus more specification is needed on the relationship between consent and age verification, and the need for concrete proportionate and reliable age verification solutions.

Chapter 5 explored the concept and the role of risk, as well as associated risk regulation mechanisms in the GDPR through a two-fold shift. It showed that the GDPR is based on an undefined and multidimensional risk notion, which is not only a potential obstacle to successfully asses and measure risks, but also might lower the protection level for individuals. In data security, risk is an objective phenomenon, which can be expressed and quantified through feared events and threats. Privacy risks are more subjective and 'individualised', and thus hard to establish, evaluate, and quantify. No uniform understanding of the privacy harms and negative impacts on individuals exists, and privacy risk are too complex to be fully caught by privacy risk management tools and methodologies.

3. Towards the future protection regime

Given the limitations of the child-specific privacy protection regime identified earlier, this section pulls together the recommendations made in different chapters of the dissertation showing how the regime can be improved. In doing so, this section answers the last research sub-question: What are ways to improve the child-specific online privacy protection regime?

3.1. Improvement of the GDPR consent mechanism

Given the weaknesses of consent in general and parental consent in particular (Chapter 3), the GDPR places an excessive burden on parents and children to make informed decisions about their personal data processing in the complex technology and data-driven environment. Instead of or in addition to asking parents to control children's data collection through consent, restrictions on the most undesirable data processing practices in relation to children should be enforced. Effective GDPR restrictions on children's data collection such as prohibition of profiling, marketing, the use of legitimate interest as a ground to process children's data, may provide an alternative to the parental consent requirement as a protection model. Purpose dependent restrictions on the collection of children's data would be better suited to diminishing its commercial exploitation in complex marketing, tracking and targeting systems, than parental consent.

Given that consent has been assigned a prominent role in the GDPR, when data processing is based on the parental consent it could be fine-tuned as a protection mechanism. As regards the age threshold for consent, it might be worth adopting different age limits for different data collection areas and practices in the 13–16 year age span. Specific consent age limits could be determined in national laws as Member States can depart from the GDPR default age of 16 or in codes of conduct at the European level. The latter could help to create standards that account for children's vulnerabilities in a specific activity or sector. If the Member States chose to lower the age threshold to 13, the industry codes of conduct could still go beyond this age requirement and guarantee stringent protection in specific data collection scenarios offering more protection for children's personal data depending on the context. In any case, the choice of the most appropriate age limit between 13 and 16, be it in national law or in self-regulatory initiatives, should be based on extensive empirical evidence and consultations with children.

The implementation of Article 8 of the GDPR provides an opportunity for the EU to address the different challenges and opportunities in adopting innovative online methods of age verification. Instead, of purely relying on the internet users' self-assertion of their age, as provided in the COPPA regime in the US, the EU should explore innovative, effective and privacy-friendly age verification mechanisms, aligning them with the advancements in online authentication, attribute-based ecosystems and public e-ID schemes. The use of attribute-based credentials in implementing Article 8 of the GDPR looks particularly promising, allowing for pseudonymous and reliable age checks online. In line with the risk-based approach embodied into the GDPR, methods of age verification that afford lower levels of assurance might be adequate in online services posing lower risks to the rights and freedoms of children, leaving high assurance options for high risk information society services, such as services involving profiling, marketing and other practises from which the GDPR considers that children merit specific enhanced protection.

When determining acceptable parental consent verification methods, the EU could follow the US example and encourage industry to propose effective, acceptable (from an industry perspective) and sector-tailored solutions for approval. Codes of conduct could be one possible way to create standards for effective consent verification and the further specification of Article 8 of the GDPR. Nevertheless, in order to ensure that self-regulation is accountable, efficient and able to deliver on its societal goals, the EU should actively participate in the formulation of self-regulatory rules, and their effective monitoring and enforcement.

3.2. Child-tailored risk assessments: taking children's interest, needs vulnerabilities into account

In order to take into account the specific catalogue of fundamental rights and freedoms (i.e. the UN Convention on the Rights of the Child) and the earlier identified reasons to protect children (special needs and vulnerabilities), Chapter 6 proposed to conduct the child-specific DPIAs. It first discussed the general criteria of DPIAs established in Article 35 of the GDPR: the envisaged processing operations and their purposes of the processing, the necessity and proportionality of the processing, the impact on the rights and freedoms of data subjects. As a case study, it focused on the PRIAM methodology and showed how its components, categories and attributes can be specialized in the context of a child-specific DPIA assessing risks for children in the information society context (online privacy risks).

3.3. Holistic understanding of the GDPR concepts and principles: lessons from consumer law

Chapter 4 explored the extent to which EU consumer law, which takes account of children as a particularly vulnerable group of consumers, can inform the GDPR and reduce the clarity gap in relation to some GDPR concepts and principles, principles of fairness, transparency, and conceptual questions of an average child and services directed to children.

Bearing in mind consumer law and the requirement to provide clear and comprehensive pre-contractual information to consumers, icons and symbols, personalized information and participatory transparency have been considered as the ways to implement child-adapted transparency in data protection law. It has become clear that the proposal of personalized information, although promising and interesting from a consumer law perspective, as a transparency mechanism cannot be easily aligned with the core data protection requirements as its implementation requires the profiling of children. It is also questionable if and to which extent icons, pictograms and other non-verbal ways of transmitting information can be effective and feasible for the implementation of the GDPR in relation to children.

Relying on consumer protection, the GDPR could be interpreted as forbidding a priori some unfair and undesirable data collection and use (e.g. personalisation) practices. Consumer law would also allow to establish violation of fairness even in cases where the child or his representative has consented to the processing. In addition, the blacklist contained in Annex 1 in the Unfair Commercial Practices Directive could be updated to include a list of unfair commercial data-processing practices in order to ban them as misleading or aggressive.

Consumer law can provide guidance on how to interpret definition of information society services offered directly to a child allowing to include services not only directly targeting children but also those that are likely to appeal to children due to their content, style and presentation. Finally, following the logic of the Unfair Commercial Practices Directive, the GDPR could rely on an average data subject, define an average child in different data

collection scenarios and explore the correlation between the characteristics of certain age groups of children and the likelihood of being vulnerable for specific commercial data collection practices.

3.4. Improved self-regulation

In line with the broad definition of regulation employed in this dissertation, Chapter 7 looked beyond hard law and included into the regulatory regime the current self-regulatory rules for the online privacy protection of children. It drew on two different areas: online child safety and online advertising and analysed four self-regulatory initiatives: the Safer Social Networking Principles, the CEO Coalition's Statement of Purpose, the ICT Coalition's Principles, and the FEDMA code. At the time of writing, these were the only existing self-regulatory initiatives dealing with online child privacy as a substantial part of their content.[1003]

The chapter focused on the procedural (rule formulation, monitoring, enforcement) and organizational (organizational structures, role of public actors) aspects of the initiatives, and demonstrated significant limitations of self-regulation in the area of online child safety compared to the area of online advertising. The former suffers from limitations due to broadly formulated statements and unmeasurable commitments, limited monitoring mechanisms and often non-existent sanctions. The comparison provides an opportunity to distinguish several features that can possibly contribute to greater effectiveness of the self-regulatory schemes to protect the online privacy of children.

First, clearly defined voluntary rules and measurable standards, rather than a broad statement of objectives, can enable better adoption and action of the voluntary initiatives in practice. In addition, formal approval of the industry formulated rules by public authorities can help to take into account public interests. However, it has been recognized that refined and detailed rule-making is possible when the rules aim to mitigate a single privacy risk, such as personal data misuse. Online child safety initiatives, where different risks and various aspects of social privacy are at stake, require multi-stakeholder dominated platforms which manage to agree only on broad statements and principles. They can hardly be prescriptive and provide technical implementations, as they inherently focus on desired outcomes, leaving a large margin of maneuver for implementation to individual companies. As a result, their adoption and implementation is inevitably more complicated and less measurable.

Second, the lack of independent monitoring schemes and the absence of enforcement mechanisms and dissuasive sanctions in cases of malpractice in the majority of the online child safety initiatives could be mitigated by the availability of organizational structures for self-regulatory tasks. An industry association of a particular sector, through "institutionalization" of self-regulation, would not only provide the necessary personnel and organizational structures to enforce self-regulatory rules and impose fines for non-compliance, but also due to the additional benefit provided to its members, such as lobbying, education and training, could exercise a threatening power in case of exclusion. However, such stable structures do not exist yet in cases where multi-sectoral action to mitigate online privacy and safety risks is necessary.

[1003] Since the article has been published, one of the self-regulatory initiatives (the CEO Coalition) ceased to exist and a new initiative (the Alliance to better protect minors online) has been launched. In the Statement of Purpose, adopted on 7 February 2017, the Alliance members agreed to curb harmful content, conduct and contact, through three strands of action: user-empowerment to promote enhanced use of online safety tools, cooperation and sharing of best practices, awareness raising and access to positive, educational and diversified content online. (at: https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids)

Therefore, it has been argued that it would be more beneficial to tackle online child privacy issues separately from safety initiatives and use sectorial industry associations for the self-regulatory task. This would not only bring online privacy protection mechanisms more in line with the human rights perspective, but also lead to clear and more enforceable rules given the possibility for public authorities to approve their content and the similarity of the industry players. Such a human rights-based approach, instead of a safety-based approach, would consequently require the EU to take a stronger and better defined co-regulatory strategy. The new General Data Protection Regulation envisions a similar future and encourages associations to adopt approved and monitored codes of conduct for the purpose of specifying the application of data protection provisions when processing children's personal data.

4. Future research directions

This dissertation aimed at researching how the EU law and self-regulatory initiatives can protect children from online privacy risks while accounting for the particular characteristics of children. At the moment of completion of this dissertation, which was written in the middle of academic debates of theoretical and practical justifications as well as policy developments in the area of children's online protection, a number of issues have been identified for future research and will be presented in this section with the hope that they will be the starting point for fruitful academic debates and inspiration for further research.

In answering its main research question, the dissertation takes a child rights-based theoretical approach. It sheds light on some of the tensions and complexities that arise when this approach in applied in an attempt to ensure online privacy for children. Recent developments in online privacy protection for children in the European Union and in particular the specific provisions of the GDPR, as discussed in this disseration, create a new level-playing field in Europe. Future research is needed to assess in detail how the child rights-based approach and the lenses of protection, participation and provision it promotes, could still contribute towards the safeguarding the online privacy of children and help to interact in harmony with other child rights foreseen in the UN CRC. Future research is also necessary in order to examine how certain concrete data-driven daily practices impact the rights of children. For example, as noted by Lupton and Williamson,[1004] big data may potentially lead to direct contravention of Article 12 UN CRC, and instead of engaging children to express their views and perpectives, actually silence their voices.

The research identified the need for more empirical data on children and privacy online, including privacy related harms stemming not only from the interactions between individuals but also, increasingly importantly, from commercial data collection and use, should be gathered. In the context of privacy and data protection, such information is indispensable for instance in the context of data protection impact assessments. Despite the methodological and ethical challenges that the research will have to overcome,, the empirical research on harms is a stepping stone for policy making. As acknowledged by Slavtcheva-Petkova et al. "a focus on risk, or the risks of risk to the exclusion of harm is ultimately self-defeating, for without research into the types of harm experienced, we cannot know who is at risk, or why that should matter, and may fail to notice certain new or emerging sources of concern"[1005].

[1004] Deborah Lupton and Ben Williamson, The datafied child: The dataveillance of children and implications for their rights **,** *New Media & Society* Vol 19, Issue 5, pp. 780 - 794

[1005] Vera Slavtcheva-Petkova, Victoria Jane Nash & Monica Bulger, Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research, Information, Communication & Society Vol. 18 , Iss. 1,2015, 60.

There is a need for future research on children's privacy online and related harms to pay more attention to specific age groups, instead of relying on the general distinction between children and adults. As discussed in Chapter 4, policy makers should explore different sectors, data collection practices and age groups, for example by looking into the correlation between the characteristics of certain age groups of children and the likelihood of being vulnerable for specific commercial data collection practices. In line with the 'evolving capacities' of the child, identified in Article 5 of the UN CRC and the recent General Comment No. 20 on the Implementation of the Rights of the Child in Adolescence adopted by the Committee on the Rights of the Child,[1006] approaches in data protection law in relation to adolescents should differ from approaches to younger children in order to realise their rights and recognise their development, increasing capacity and agency and the implications for consent.[1007]

Finally, an underdeveloped field that would reguire further exploration is the involvement of children in regulation and policy making. It is well established that the views of children themselves should be considered in policymaking and the preparation of national laws related to the use of children's personal data, as well as in their evaluation.[1008] As noted by the Committee on the Rights of the Child, 'including children should not only be a momentary act, but the starting point for an intense exchange between children and adults on the development of policies, programmes and measures in all relevant contexts of children's lives'.[1009] However, currenlty children do not have a voice on the regulation of issues that relate to them and no public consultation has taken place to incorporate their voice, even if the GDPR directly affects children's rights and interests.

[1006] General comment No. 20 (2016) on the implementation of the rights of the child during adolescence CRC/C/GC/20, 6 December 2016.
[1007] Berman, G. and Albright, K. (2017). Children and the Data Cycle: Rights and Ethics in a Big Data World, Innocenti Working Paper 2017-05, UNICEF Office of Research, Florence.
[1008] Committee on the Rights of the Child, The right of the child to be heard (General Comment No. 12) (2009) CRC/C/GC/12.
[1009] Ibid., 5.

Summary

The dissertation examined EU data protection law and self-regulation initiatives and questioned how they can be protect children from online privacy risks while accounting for the particular characteristics of children. It proposed to include the specific catalogue of fundamental rights and freedoms (i.e. the UN Convention on the Rights of the Child) and account for special needs and vulnerabilities of children in the child-specific data protection impact assessments. Also, it showed that the child-specific data protection regime can benefit from more legal certainty if consent, as a protection mechanism, is fine-tuned drawing on the US COPPA's experience, and the GDPR concepts and principles, (principles of fairness, transparency, and conceptual questions of an average child and services directed to children) are interpreted holistically with the EU consumer law. Finally, it claimed that the regime could become more effective and bring online privacy protection mechanisms more in line with the human rights perspective if online child privacy risks were addressed separately from safety risks, preferably in the self-regulatory codes of sectorial industry associations. This could lead to clearer and more enforceable rules given the possibility for public authorities to approve the content of such codes and the similarity of the industry players.

Annex 1: Overview of the survey results

No.	Country and respondent	SPECIFIC LEGAL PROVISIONS (until 2014)	COMPLAINTS (2009-2014)	COURT DECISIONS (until 2014)	SOFT LAW AND OTHER INITIATIVES Other initiatives (until 2014)
		1. Does your country have specific legal provisions regulating the protection of children's (age below 18) personal data online? If yes, please specify and provide references to the relevant legal acts.	*2. How many complaints related to the infringement of children's privacy/data protection rights online did your data protection authority (DPA) receive in the last 5 years (please, if possible, specify the amount of complaints per year since 2009)? How many of the received complaints resulted in an action of your DPA? What were the reasons for complaints and the adopted decision of the DPA? Please provide reference to the relevant texts.*	*3. Are there any court decisions relating to the infringement of children's privacy/data protection rights online? Please provide reference to the relevant court decisions.*	*4. To your knowledge, are there any soft law instruments (codes of conduct, guidelines, principles, etc.) adopted on the national level aiming to protect children's personal data online? Please provide a reference to the relevant texts.* *5. If possible, please provide any other relevant information (documents, reports, surveys, etc.) you are aware of in light of the research topic.*
1.	**Austria**	No specific legal provisions.	No complaints received.	No court decisions.	No soft law and other initiatives.
2.	**Belgium**	No specific legal provisions. Belgian DPA has issued an Opinion No. 38/2002 on the protection of privacy of minors on the internet.[1010]	Statistical information is not detailed enough to answer the question.	The DPA has no information about such decisions.	<u>Initiatives of the DPA:</u> Long-term awareness raising initiative "I decide" on modern technologies and their impact on privacy.[1011] The DPA aims to educate children and young people about the importance of privacy and responsible

[1010] Opinion No. 38/2002 of 16 September 2002 concerning the protection of the private life of minors on the Internet, available at: https://www.privacycommission.be/sites/privacycommission/files/documents/advies_38_2002_0.pdf (Dutch); https://www.privacycommission.be/sites/privacycommission/files/documents/avis_38_2002_0.pdf (French)

[1011] Website of "I decide" initiative is available in Dutch (http://www.lkbeslis.be) and French (http://www.Jedecide.be). The description of the initiative provided by the DPA: "The Belgian DPA has its own "I decide" project, for which its original ambition was to act as a knowledge centre, to make its know-how, experience and services available to the world of education and other organisations working with and for young people. The objective of the DPA throughout the project has been to raise awareness on the importance of privacy for young people, because they do not always realize that rapid technological developments and the temptation to use technology intensively result in the dissemination of their personal data. However, the DPA did not want its message to be a "heads up" stressing dangers instead of possibilities: the Belgian DPA only aims at reconciling young people's privacy with the positive impact of modern technologies, in order for them to take their own well-informed decisions on whether or not they disclose their personal data. 'I decide - young and aware of my privacy' is a powerful statement, launched by the Belgian DPA approximately five years ago as the title of a long-term initiative aimed at awareness raising among young people on all possibilities of modern technologies and their impact on privacy."

					behaviour online without stressing dangers instead of possibilities.
3.	**Bulgaria**	No specific legal provisions.	No complaints received. In May 2011, the DPA was asked for an opinion by another public authority on whether the IP address is personal data in a case related to a website which disseminated erotic pictures of children.	The DPA has no information about such decisions.	Initiatives of the DPA: In 2012, the DPA organized the information campaign "Data Protection Week" (a site with information on important privacy and personal data protection issues and the leaflets were created).[1012] A competition "Me and the Internet" for drawings, essays or poems on the dangers of the internet and the importance of the personal data protection online. 60 children (4-17 years of age) took part in the competition. Other initiatives: - The Bulgarian Safer Internet Node (http://safe.teacher.bg/html/etusivu.htm in Bulgarian) - State Agency for Child Protection publishes documents in the area of "Children in the information society" (http://sacp.government.bg/deinosti/deca-info-obshtestvo/- in Bulgarian)
4.	**Croatia**	No specific legal provisions.	The DPA received 55 complaints on the misuse of children's personal data. 4 complaints exclusively related to the personal data processing online, others to data processing by newspapers (including online versions), media and preschool public institutions. In each of the cases the DPA took measures to protect the child rights.	The DPA has no information about such decisions.	Initiatives of the DPA: Together with the Centre for Safer Internet (http://www.sigurnijiinternet.hr/) the DPA promotes protection of children's online privacy. Other initiatives: - Red Button Project by the Ministry of Interior: https://redbutton.mup.hr - Safety and Protection on the Internet project by the Polytechnic of

[1012] The texts offering guidance for children and parents when providing personal data on the Internet can be found in English on the DPA's website:
http://www.cpdp.bg/en/index.php?p=element&aid=425 - guide for children
http://www.cpdp.bg/en/index.php?p=element&aid=426 - guide for parents

					Zagreb: http://sigurnost.tvz.hr
5.	**Cyprus**	No specific legal provisions.	No complaints received.	The DPA has no information about such decisions.	To the knowledge of the DPA, there are no soft law instruments.
6.	**Czech Republic**	-	-	-	-
7.	**Denmark**	No specific legal provisions.	Statistical information is not detailed enough to answer the question.	The DPA has no information about such decisions.	The DPA has no information about soft law instruments and other initiatives.
8.	**Estonia**	No specific legal provisions.	Statistical information is not detailed enough to answer the question. Cases involving children's privacy breaches online are rare and dealt with very fast.	The DPA has no information about such decisions. Usually matters concerning children are resolved before court.	Other initiatives: Targaltinternetis.ee[1013] is an Estonian website dedicated to teaching children about online dangers and behaviour.
9.	**Finland**	No specific legal provisions.	Statistical information is not detailed enough to answer the question. There have been few cases about pictures or names of minors on the Internet.	The DPA has no information about such decisions.	Other initiatives: An organization called "Mediakasvatus- ja kuvaohjelmakasvatuskeskus" organizes events on media skills and how to use the Internet for school age children in schools[1014]
10.	**France**	No specific legal provisions. The CNIL has not adopted any decisions regarding minors in particular, but published articles on how to protect information on social media[1015] and photos online[1016]. In 2013, the CNIL proposed to amend the French Data Protection Act, and amongst others, to provide particular protection for minors	Statistical information is not detailed enough to answer the question. In 2014, more complaints on behalf of minors than in previous years were received. The subject of most of the complaints was the right to be de-indexed.	No court decisions that specifically deal with children's online data. Some cases take general children's rights into consideration (e.g. Appellate Court of Nancy, *Poirot c. SA Banque CIC* [2014, No. 362/14, 13/01512[1019]]).	Initiatives of the DPA: The CNIL puts much effort into a Digital Education programme which targets minors, e.g. the CNIL has a website dedicated to young people, parents, and educators[1020]. This website offers information for young people, parents and educators—to help understand data protection.[1021]. In coalition with EDUCNUM, the CNIL has launched a competition regarding

[1013] http://www.targaltinternetis.ee/?lang=en (in English)
[1014] https://kavi.fi/fi/kansallinen-audiovisuaalinen-instituutti/mediakasvatus-ja-kuvaohjelmayksikko (in Finnish)
[1015] CNIL, Maîtriser les informations publiées sur les réseaux sociaux, 10 janvier 2011, at: http://www.cnil.fr/linstitution/actualite/article/article/maitriser-les-informations-publiees-sur-les-reseaux-sociaux/
[1016] CNIL, Les conseils de la CNIL pour mieux maîtriser la publication de photos, 13 octobre 2014, at: http://www.cnil.fr/nc/linstitution/actualite/article/article/les-conseils-de-la-cnil-pour-mieux-maitriser-la-publication-de-photos/
[1019] Appellate Court of Nancy, 10 février 2014, *Poirot c. SA Banque CIC*, arrêt n° 362/14, 13/01512
[1020] http://www.jeunes.cnil.fr/
[1021] Guidelines available at: http://www.jeunes.cnil.fr/espace-jeunes/mon-quotidien/;

		online[1017] by enhancing children's rights to effectively erase their online personal data.[1018]			Digital education. According to the CNIL: "the idea is to get students thinking about how to best transmit good reflexes and good practices regarding personal data online to children and young people[1022]. In other words, instead of a regulator deciding how to best inform the youth, it will be a "youth to youth" discussion model. Thus, the youth will come up with new and inspiring ideas on how to best educate the next generation."
11.	**Germany**				
	Rheinland-Pfalz Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz	The protection of children's rights in Germany is regulated in the "Jugendschutzgesetz", a federal law, which does not contain any specific regulations on children's personal data. Each of the 16 federal-states has its own data-protection-law. The data protection law of Rhineland-Palatinate does not contain any specific provisions on the protection of children.	Statistical information is not available to answer the question.	No court decisions in the area of DPA's responsibility.	No soft law instrument on national level on children's privacy. Other initiatives: An institution called "jugendschutz.net" focuses on protection of children and youth in general.
	Brandenburg Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg	We are not aware of any separate rules for the protection of personal data of children in the online area. General rules for the data protection of children and adolescents can be	3 concrete complaints regarding the handling of personal data of children and young people on the Internet have been received: 2010 - Publication of student names on lists that document payment for a class trip;	No court decisions in the area of DPA's responsibility.	Initiatives of the DPA: No concrete instructions on the subject have been issued by the DPA. However, the DPA carries out information and teaching events on data protection in schools for pupils and teachers. It has also conducted teaching

[1017] CNIL, Présentation du 3'ème rapport d'activité 2013, Press Conference, 19 March 2014, at: http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/Dossier_de_presse_rapport_d_activite_2013.pdf; p. 18

[1018] The proposition of CNIL has resulted in an amendment of the French Data Protection Act of 1978 (Article 40 establishes an "accelerated data erasure procedure", the condition of being a minor is sufficient to obtain the erasure of data "as soon as possible"; Article 58 foresees a possibility for the minor from 15 years old to exercise his/her rights of access, rectification and opposition and to refuse to allow his/her parents to be informed and have access to his/her personal data)

[1022] More information available at: http://www.educnum.fr/

		found in the School law of the state of Brandenburg as well as in the corresponding data protection regulation of the school system.	Pictures published on the school's website. 2011 - Publication of exam grades including the student names on the Internet. No regulatory measures were taken by the DPA in the aforementioned cases. The schools were informed about the violations and terminated them.		courses in teacher training institutions.
	Baden-Württemberg Der Landesbeauftragte für den Datenschutz Baden-Württemberg	While the State Data Protection Act of Baden-Württemberg (LDSG) regulates the processing of personal data (including minors) by public authorities based in Baden-Württemberg, the Federal Data Protection Act (BDSG) applies to the processing of personal data (including minors) by non-public authorities based in Baden-Württemberg. Neither the BDSG nor LDSG contain any specific provisions on minors. An exception is the provision on consent in § 4a (1) BDSG. Pursuant to § 4a (1) BDSG, consent is only valid if it is based on the data subject's free decision. Minors can give consent in accordance with § 4a BDSG if they are able to foresee the consequences of using their data in the respective context and therefore make a binding statement (comprehension ability). This also applies if data is collected or transmitted online.	Statistical information is not available to answer the question.	The DPA has no information about such decisions	-

		In public schools in Baden-Württemberg, the use of social networks for communication, e.g. between teachers and students is prohibited by a guide of the Ministry of Culture[1023].			
	Mecklenburg - Vorpommern Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern Heinz Müller	No specific legal provisions.	No complaints received.	No court decisions.	-
12.	**Greece**	No specific legal provisions.	Relevant complaints were mainly received by telephone and answered ad hoc. Statistical information is not detailed enough to answer the question. In 2013, there has been a written complaint from a divorced mother who saw the photo of her minor child (whom she has the sole custody) posted by the father on his Facebook page without her consent. The DPA sent a letter to the father informing him that, since access to the posted material is not confined to his "Friends" but can be seen by a large number of third party contacts or may be generally accessible to all users of the service, the processing falls within the scope of the	The DPA has no information about such decisions.	Initiatives of the DPA: The DPA contributes to the protection of children's privacy online with informative seminars at schools, webinars aimed at schools all over Greece, publications and the microsite "Young Citizens".[1025] Other initiatives: Internet safety websites: http://www.saferinternet.gr/ http://internet-safety.sch.gr/ http://www.safeline.gr/

[1023]The Guide is available at: http://it.kultus-bw.de/,Le/Startseite/IT-Sicherheit/soziale+Netzwerke

[1025]More information available at: http://www.dpa.gr/portal/page?_pageid=33,97846&_dad=portal&_schema=PORTAL (in Greek)

			Greek Privacy Law 2472/1997. [1024]		
13.	**Hungary**	3 specific acts regulate the protection of children's personal data online: - Act CVIII of 2001 on Electronic Commerce and on Information Society Services (*Section 4/A.)* - Act C of 2003 on Electronic Communications *(Section 149/A)* - Hungarian Privacy Act: Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information *(Section 6, sub-section 3)*	19 cases related to the infringement of children's online data protection rights. The reasons for the complaints: the grounds of infringement of privacy rights of children, an infringement relating to children's personal data or concerning the exercise of the rights of access to public information or information of public interest, or if there is imminent danger of such infringement. Specific complaints related to issues like deletion of photos of children from social network sites, requirement for authorization of accessing website by children, conditions of publishing photos of children on internet, deletion of personal data of children from websites. In 9 out of 19 cases an administrative proceeding for data protection were launched[1026] and 2 out of these 9 cases ended with court decisions.[1027]	Court decision No. 11.K.33.918/2013 /8[1028] against a dating site nolrandi.hu due to the fact that a large percentage of the subscribers are below 16 years. The site nolrandi.hu did not have transparent terms and conditions and did not implemented technological code for setting an age limit when creating an account to prevent that children below the age of 16 can subscribe.	Initiatives of the DPA: A study published by the DPA, which promotes the conscious internet use of children.[1029] Other initiatives:[1030] - Media Literacy Education Centre Magic Valley: (http://magicvalley.hu/) - Internet Hotline: (http://internethotline.hu/tart/index/72/Erdekes_cikkek_tanulmanyok) - The Kék Vonal Child Crisis Foundation: (http://www.kek-vonal.hu/index.php/en/projects) - Safer Internet project: http://saferinternet.hu
14.	**Ireland**	-	-	-	- -

[1024]The DPA also noted that the posting and publication of a photograph of a child on a website is a decision which must be taken jointly by the parents, who exercise parental authority over minor children (cf. decision no. 34697/2010 of the Court of First Instance of Thessaloniki).

[1026]The DPA is entitled to launch a procedure if it is presumed that the illegal processing of personal data concerns many individuals; concerns special data, or significantly harms interests or results in the risk of damages. (Section 60 of the Hungarian Privacy Act)

[1027]The relevant texts related to the Authority's decisions (in Hungarian language) are: Case No. NAIH-798-40/2013/H (at:http://www.naih.hu/files/798_2013_hatarozat.pdf), Case No. NAIH-799-8/2013/H (at: http://www.naih.hu/files/799_2013_hatarozat_anonim.pdf), case No. NAIH-805-5/2013/H (at: http://www.naih.hu/files/805_2013_hatarozat.pdf).

[1028]Court decision No. 11.K.33.918/2013/8, available at: http://www.naih.hu/files/798_2013_itelet.PDF

[1029]Available at: http://naih.hu/files/projektfuzet-angol-web.pdf

[1030]Additional references to specific websites include: http://gyermekbarat.kormany.hu/csendben-van-de-biztonsagban, http://www.azinternetnemfelejt.hu/, http://neked8.mediaunio.hu/neked8/tanar/hasznos-tudas/#.U9oKEaP3zXQ

15.	**Italy**	No specific legal provisions on the protection of children's personal data online. The following provisions relate to children as data subjects more generally: a) in respect of processing operations for purposes of justice, specific safeguards are provided against the dissemination, including online, of information related to children involved in judicial proceedings. (sec. 50 and 52.5 of the Data Protection Code)[1031]: b) the Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities which is attached to the Data Protection Code, sets forth specific provisions to protect children in the journalistic field (including with respect to online journalism). In particular, Section 7 of the Code of practice gives a strengthened protection to the child's right to privacy which takes precedence over both freedom of expression and freedom of the press.[1032] This code of conduct has a	Statistical information cannot be provided. The greatest part of complaints/reports received by the DPA on processing of children's personal data concerns the publication (including online) of personal information/images related to minors by newspapers,[1033] as well as by social networking users. For example, a complaint was lodged by a woman against the dissemination, by her husband on his personal blog, of personal data related to her and her daughters. In order to reconcile freedom of expression with the right to privacy of the persons concerned the DPA ordered the anonymisation of the personal data related to the woman and her daughters.[1034] Another complaint related to an unlawful publication of sensitive personal data of a minor (a video on Youtube where a face of seriously sick girl could be clearly seen).[1035]	A ("Vividown" case) related to data processing on the Internet, i.e. the uploading on the Google video platform of a video in which a disabled minor was humiliated by his classmates. The Italian Supreme Court (decision No. 8611/2013) published the reasoning for its verdict of acquittal for the three Google executives who were sentenced to six months in prison by a first instance judgment. The Supreme Court held that Internet host providers cannot be criminally liable in cases of violation of privacy (Section 167 of the Privacy Code) due to videos (in this case of a minor) posted on the web.	Soft law instruments: - The Code of Practice Concerning the Processing of Personal Data in the Exercise of Journalistic Activities. - The "Treviso Charter", a set of principles specifically aimed at protecting children's privacy and dignity. Such Charter, in cooperation with the DPA, was updated in 2006 in order to extend children' protection also to online journalism.

[1031] http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf
[1032] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1565746
[1033] E.g. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3726124; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2957346; http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3403030
[1034] Available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3117705
[1035] Available at: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2923201

		particularly stringent value since the respect of its principles is a pre-requisite for the processing to be lawful, as foreseen by Article 12 of the Data Protection Code.			
16.	**Latvia**	No specific legal provisions.	Statistical information is not available. The DPA received several complaints related to children's data published online (e.g., results of competitions indicating name, surname and other personal data of children; the height and weight of identifiable children published online by a Model school) or information provided to third parties without a legal ground (e.g., a characteristic of certain identifiable child provided to third persons).[1036]	None of the DPA decisions regarding the children's personal data protection has been challenged in court. The DPA has no information about other decisions.	Initiatives of the DPA: A recommendation issued by the DPA "Children's Personal Data Protection in Schools".[1037] Other initiatives: Informative materials regarding children's rights online by the State Inspectorate for Protection Of Children's Rights[1038]
17.	**Lithuania**	No specific legal provisions.	No complaints received. The Office of the Inspector of Journalist Ethics examines complaints (applications) of interested persons with regard to personal data violations in the media and could have received relevant complaints.	The DPA has no information about such decisions.	The DPA has no information about any relevant soft law instruments.
18.	**Luxembourg**	No specific legal provisions.	14 complaints regarding specifically children's privacy/data protection rights were received. Most of those complaints concerned	The DPA has no information about such decisions.	Other initiatives: BeeSecure (https://www.bee-secure.lu/) organises and promotes the secure use of

[1036] According to the Children's Protection Law in Latvia the cases concerning children should be considered as a priority by each state institution, thus also by the DPA. Therefore there has always been an action from the DPA, including fines applied for illegal data processing.
[1037] The recommendation is available at: http://www.dvi.gov.lv/lv/jaunumi/publikacijas.
[1038] Available at: http://www.bti.gov.lv/lat/informativie_materiali/bukleti/).

			pictures/photographs/films of children published via various media on the internet (Facebook, internet sites and blogs, Youtube, etc.), some concerned requests for deletion of accounts created by minors (PayPal, Amazon, etc.) and identity theft cases. All of those cases were investigated and relevant action was taken accordingly.		the internet and other media, especially for young people.
19.	**Malta**	-	-	-	-
20.	**Netherlands**	The Dutch data protection act specifies in Article 5(1) that children under 16 cannot give valid consent. This rule applies to all types of data processing for which consent is the legitimate ground, including online data processing. In 2007, the Dutch DPA has published Guidelines on the publication of personal data on the internet, with many examples about minors.[1039]	The Dutch DPA receives dozens of questions and signals per year related to children's online privacy. These signals may be questions about relatively easy to answer data protection issues, or serious complaints from (legal representatives) of children about an alleged breach of their right to data protection. Compared with other data protection issues, the amount of signals and complaints the Dutch DPA receives about children's online privacy is low. Other investigations relating to children's online privacy: 2009 - Investigation social networking site www.zikle.nl aimed at children 12-15 years old 2009 - Investigation ranking & rating site beoordeelmijnleraar (school children rating their teachers) (many	The DPA has no information about such decisions.	The DPA has no information about any relevant soft law instruments. Initiatives of the DPA:[1041] The DPA provides specific guidance for the general public regarding children and online privacy on its website. Other initiatives: Work of the organisations 'Mijn Kind Online', 'Ouders Online', and Kinderombudsman.

[1039] 2007 - Richtsnoeren publicatie persoonsgegevens op internet (also available in English, Guidelines for the publication of personal data on the internet, with special attention for minors, see: http://www.dutchdpa.nl/downloads_overig/en_20071108_richtsnoeren_internet.pdf).

[1041] The Dutch DPA has actively contributed to a number of opinions from the Article 29 Working Party and the Berlin group of data protection experts relating to internet issues. All of these opinions contain specific recommendations with regard to children's online privacy. See specifically the opinions on Mobile apps (2013), Online behavioural advertising (2010), Online social networking (2009) and Search Engines (2008), Working Document 1/2008 on the protection of Children's Personal Data and the Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" – (Rome (Italy), 3./4.03.2008) of the Berlin Group.

			signals/complaints received in 2008) 2009 - Investigation tell-a-friend game website jiggy.nl aimed at children.[1040]		
21.	**Poland**	No specific legal provisions.	No relevant administrative proceedings conducted.	-	Initiatives of the DPA: A survey "*The perception of issues related to data protection and privacy of children and young people*" has been conducted. Together with the survey results the DPA published tips and recommendations on how to protect personal data and privacy while using the Internet.[1042] From 2009 the DPA conducts an educational programme "*Your data – your concern. Effective protection of personal data. Educational activity addressed to students and teachers*".[1043]
22.	**Portugal**	No specific legal provisions.	Statistical information is not available. The reasons for complaints are related to the abusive disclosure of personal data (e.g. on school websites or photos in social media networks). The DPA has applied fines and ordered the erasure of the data.	The DPA is not aware of such decisions.	The DPA is not aware of any soft law. The DPA plans to develop specific guidelines for the data processing in the school context, including the online world. Initiatives of the DPA: The DPA developed an awareness raising project for children at school (DADUS Project) to provide information on data protection and privacy, safe ICT use,

[1040] Other investigations conducted by the Dutch DPA relating to information society services are also likely to involve children, e.g. the investigation into the data processing by the app WhatsApp, or the investigation into data processing by Google after the change of its privacy policy in May 2012.

[1042] These guidelines are addressed to parents and teachers. The main result of the research is that actions which aim is to raise awareness in the field of personal data and privacy protection among children and youth in the online environment are absolutely essential in order to protect them in the Internet and remind them about the need to protect privacy because they do not always remember about it, sharing carelessly their personal data while using the Internet. The survey is available at the DPA's website http://www.giodo.gov.pl/1520124/id_art/6914/j/pl (in Polish).

[1043] During the 4th edition of the programme, teachers from schools involved in the initiative developed lessons' scenarios devoted to the education in the field of personal data and privacy protection also on the Internet. This material, written in Polish, is restricted to the participants of the programme.

					online risks and ways to minimize them.[1044]
23.	**Romania**	No special legal provisions.[1045] Before processing personal data of minors aged between 14 and 16, their agreement and parental consent should be obtained.[1046]	No complaints received.	The DPA is not aware of such decisions.	Other initiatives: The Sigur.Info project (www.sigur.info) on the promotion of the use of the internet and of the new online technologies in the safest conditions, Safer Internet plus. Two brochures - "Practical Guide for Teenagers" and "Practical Guide for Parents" are also available in Romanian.[1047]
24.	**Slovakia**	No special legal provisions.	No complaints received.	The DPA is not aware of such decisions.	Other initiatives: The telecommunication companies have special departments or sections on their websites dealing with children's protection. Several NGOs in Slovakia are working on this subject: (e.g. the website www.zodpovedne.sk on protection of children online, a civil association eSlovensko, the project "Ovce" (Sheeplive)). The DPA is of "the opinion that the parents and children in Slovakia have enough information on the issue of children's protection in the net. Children have also subject of "information

[1044] This Project was launched in 2008 with great adhesion from schools (teachers and pupils) and the support of the Ministry of Education, through a cooperation protocol. The Project worked based on a e-platform and all kind of materials were developed by the DPA. The DADUS Project is now under revision, evolving to a different role, as the Ministry of Education has officially inserted data protection and privacy issues in the curricular programmes of the ICT discipline, which is mandatory for all children for two years.

[1045] The provisions of Law No. 677/2001 are applicable and the provisions of article 12 of Law no. 506/2004 on the processing of personal data and protection of private life within the electronic communication's sector must be taken into account. As regards the operations of collection of minors' personal data via the internet, these are susceptible to present special risks for their rights and liberties and for that reason data controllers must bear in mind ensuring an efficient protection for minors. One must also take note of the legal provision which guarantees children's right in relation to protecting their public image, the intimate, family and private life, the protection against any forms of exploitation or abuse, etc.

[1046] The legal system of Rumania recognizes a restrained capacity for the minors aged between 14 and 16. It is necessary to obtain minors' agreement, as well as the consent of their legal representatives for personal data processing. Therefore, depending of the minor's age, their legal representatives may be required to provide their contact data (phone number, e-mail, etc.) in order to allow for them to be contacted or, alternatively, the use of certain applications oor enrolment on various websites may be conditioned to only being done by the parents. In all situations, the fact that minor's legal representatives have given their express and unequivocal consent must be provable.

[1047] They aim to describe the types of situations which may catch children unprepared as well as the types of illegal or harmful content on the internet, which must be reported to the Safenet.ro hotline.

					technologies" at school when they receive information on protection necessity. In addition to help from state authorities the green line is operated to help children with any problem and many children have used this line".
25.	**Slovenia**	No specific legal provisions.	Approximately 10 complaints regarding on children's data processing online were received. The majority of these complaints related to the publishing of children's photos online (photos taken in kindergarten, school, etc.); one complaint related to the publishing of personal data of all children born in 2010 on a municipality's webpage. In each case the DPA asked the data controller to demonstrate the legal basis for the processing of personal data. If the data controller was not able to provide a *concrete* consent of the parents, the Commissioner ordered for the data/photos to be removed.	The DPA is not aware of such decisions.	Soft law instruments: - Self-regulatory code of conduct of the public electronic communication services providers on the protection of users[1048] - Self-regulatory code of conduct of mobile operators of public electronic communication services on safer use of mobile phones by children and adolescents up to 18 years - Code of conduct on hate speech:[1049] Initiatives of the DPA: Since there are no legal instrument regulating the protection of children's personal data online the DPA (alone and together with other organizations) performs many awareness raising activities: prepares and publishes leaflets and brochures on the subject, gives lectures to children and teachers, gives advices through its non-binding opinions, etc. Soft law instruments prepared by the DPA: - guidelines Fighting cyber bullying[1050] - guidelines How to use Facebook and survive[1051]

[1048] At: http://www.ris.org/uploadi/editor/1360137260Kodeks_ravnanja_za_zascito_uporabnikov_2013.pdf
[1049] At: http://safe.si/spletno-oko/za-urednike-spletnih-mest
[1050] At: https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice-glede-varstva-pred-spletnim-nadlegovanjem.pdf
[1051] At: https://www.ip-rs.si/fileadmin/user_upload/Pdf/brosure/Kako_uporabljati_FB_in_preziveti_tisk__v2_-net.pdf

					- several non-binding opinions.
26.	**Spain**	One provision (Art. 13 of the Regulation Implementing Organic Law 15/1999, on the Protection of Personal Data, Approved by Royal Decree 1720/2007) specifically refers to children. It sets special requisites in relation to consent for the processing of personal data of children.[1052] In connection with the protection of children in this matter, it would also be necessary to take into account the provisions of the Spanish Information Society and Electronic Commerce Act (Ley 34/2002) regarding cookies (https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758).	Statistical information is not detailed enough to answer the question. Based on the experience of staff dealing with complaints, only a very limited number of complaints have been lodged before the Spanish DPA involving children´s personal data online. The cases basically were related to the absence of parental consent (or of procedure to authenticate the consent), the unlawful use of personal data of third persons (minors and adults) by children on the Internet. In one case, for instance, the complaint was related to the recording and posting in YouTube of images of a handicapped minor. These few complaints seem to reflect the existing pattern with regard to children's data processing on line. In most of the cases, and given that unlawful processing tends to be associated with criminal offences, the police and the courts are the	The DPA has no information about such decisions.	Soft Law Instruments: The Spanish DPA is responsible for registering the codes of conduct on data protection. One of them, called "Confianza Online", is aimed to the electronic commerce and the interactive advertising and includes special provisions for protection of children´s personal data online (arts. 34 – 37).[1053] Initiatives of the DPA: More information on protection of children´s personal data in the DPA website (Canal Joven) (www.agpd.es). Other initiatives: Several institutions, organizations and enterprises have made studies and surveys on this issue, including the Spanish Senate and the Spanish Congress.

[1052] *"Article 13 Consent for the Processing of Data of Minors*

1. *Data pertaining to data subjects over fourteen years of age may be processed with their consent, except in those cases where the law requires the assistance of parents or guardians in the provision of such data. The consent of parents or guardians shall be required for children under fourteen years old.*
2. *Under no circumstances may data be collected from the minor regarding information about any other member of the family unit, or about its characteristics, such as data relating to the professional activity of the parents, financial information, sociological or any other such data, without the consent of the persons to whom such data refer. The aforesaid notwithstanding, data regarding the identity and address of the father, mother or guardian may be collected for the sole purpose of obtaining the authorization set out in the previous subsection.*
3. *When processing refers to the data of minors, the information aimed at them shall be expressed in easily understandable language, with express indication of the provisions of this Article.*
4. *The data controller is responsible for setting up the procedures that guarantee that the age of the minor and authenticity of the consent given by the parents, guardians or legal representatives have been effectively checked."*

[1053] http://www.agpd.es/portalwebAGPD/canaldocumentacion/codigos_tipo/common/pdfs/codigo_tipo_confianza_online_nov_2009.pdf (in Spanish)

			institutions that currently dealt with the claims.		
27.	**Sweden**	No specific legal provisions.	Statistical information is not available.	The DPA is not aware of such decisions.	Other initiatives: Other relevant authorities in Sweden: the Swedish Media Council (http://www.statensmedierad.se/Om-Statens-medierad/In-English/) and the Ombudsman for Children in Sweden (http://www.barnombudsmannen.se/english/about-us/)
28.	**United Kingdom**	The UK Data Protection Act 1998 does not specify a particular age limit for any of its provisions with one exception. There is an exception for Scotland on the right for a data subject to access their personal data. That person must be aged 12 or over.[1054]	Statistical information is not detailed enough to answer the question.	The ICO is not aware of any decisions with regard to children's rights online specifically. There are other court decisions, however, regarding compliance with the data protection principles based on whether the personal data being processed belongs to a child or not.[1055]	Initiatives of the DPA: The ICO has a web page dedicated to young people (those under 18) which has some helpful guidance on data protection (http://ico.org.uk/youth). The ICO has also twice supported an initiative by the law firm Speechly Bircham with regard to children protecting themselves online. This initiative is called "I in Online" and helps teach children about protecting their privacy when online (http://www.theiinonline.org/).

[1054] Data subject's rights - http://www.legislation.gov.uk/ukpga/1998/29/part/II Exemption regarding rights in Scotland - http://www.legislation.gov.uk/ukpga/1998/29/section/66

[1055] R (on the application of) T -v- Chief Constable of Greater Manchester and others, 28 January 2013, available at: http://www.judiciary.gov.uk/judgments/r-t-chief-constable-greater-manchester-judgment-29012013/

Acknowledgment

This book has benefited from the generosity and insights of many people who shared their time, encouragement, and help.

First of all, I would like to thank my supervisors Corien Prins and Eleni Kosta for their guidance and support throughout the four years of my Phd trajectory, and in particular at the end of it. Dear Corien, I could not imagine a more supportive, warm and positive supervisor. Thank you for always trusting me and inspiring me as an academic and as an incredible human being. Dear Eleni, it would have been difficult without your friendly and goal-oriented guidance and support. Your excellent planning skills and concrete suggestions contributed to bringing this dissertation to completion. You always encouraged me to think critically and to express my own position. You have taught me that not only the knowledge, but also the confidence with which it is presented, matters.

I would like to express my gratitude to prof. Valerie Steeves form the University of Ottawa, who warmly hosted me for a research visit and made numerous connections. Thank you for great socio-legal discussions, and for being always so kind, happy and welcoming.

I am also grateful to the researchers from the UNICEF Office of Research - Innocenti in Florence where I spend a moth as a research fellow. In particular, I thank to Jasmina Byrne, Gabrielle Berman and Daniel Kardefelt-Winther, who provided me valuable insights and suggestions on child rights and their actual working on the ground.

I am also indebted to prof. Sonia Livingstone, prof. Eva Lievens, prof. Chris Hoofnagle, prof. Vanessa Mak and Daniel Cooper who found time to read and comment on various chapters in this book. I would like to thank prof. Simone van der Hof for her challenging and detailed comments which contributed to the improvement of the overall dissertation.

I am proud to have been part of TILT, such an excellent and vibrant research environment. In particular, I would like to thank Nadya, Maartje, Tjerk, Claudia, Michael, Mariana and Adele for their friendship, wise criticism and inspiring talks.

A special acknowledgment should go to Damian for endless discussions, detailed comments and excellent (‘ironic oxymoronic’) suggestions from which many of the paragraphs of this book have benefited.

Last but not least, I owe a debt of gratitude to my family: to Gianluca for reminding me that PhD is much more than a written book (and that ‘no dissertation is ever perfect or absolutely finished’) and to Margot and Matias for accepting me being absent when we should have been splashing together in puddles and climbing trees in surrounding playgrounds.